



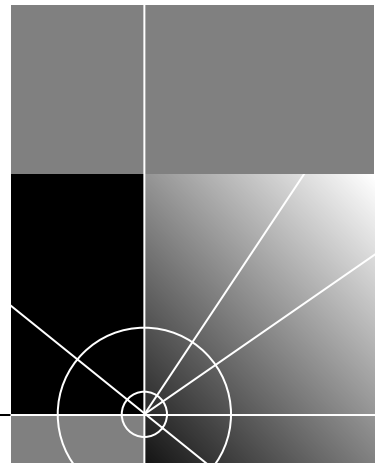
# Transcend® Traffix™ Manager User Guide

Software version 3.0 for Windows NT®

<http://www.3com.com/>

Part No. 09-1825-000  
Published August 1999

---



**3Com Corporation**  
**5400 Bayfront Plaza**  
**Santa Clara, California**  
**95052-8145**

Copyright © 1999 3Com Technologies. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Technologies.

3Com Technologies reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Technologies to provide notification of such revision or change.

3Com Technologies provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

#### **UNITED STATES GOVERNMENT LEGEND**

*If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:*

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, LANsentry, SmartAgent and Transcend are registered trademarks of 3Com Corporation. Traffix is a trademark of 3Com Corporation. 3Com Facts is a service mark of 3Com Corporation.

Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated. HP and OpenView are registered trademarks of Hewlett-Packard Company. AIX and IBM are registered trademarks of International Business Machines Corporation. Notes is a registered trademark of Lotus. Netbios is a trademark of Micro Computer Systems Inc. Microsoft, Visual Basic, Visual C++, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Java and SunNet Manager are trademarks of Sun Microsystems. Solaris is a registered trademark of Sun Microsystems. UNIX is a registered trademark of X/Open Company, Ltd. in the United States and other countries.

All other company and product names may be trademarks of the respective companies with which they are associated.

Guide written by Emma Cuthbert. Edited by Patrina Law.

# CONTENTS

---

## **ABOUT THIS GUIDE**

How To Use The Traffix Manager Documentation	11
Conventions	13
Terminology Used in this Guide	14
Related Documentation	14
Documents	14
Web Sites	14
Documentation Comments	15
Year 2000 Compliance	16

## **PART I GETTING STARTED WITH TRAFFIX MANAGER**

---

### **1 TRAFFIX MANAGER OVERVIEW**

What to Read First	19
Features of Traffix Manager	20
How Does Traffix Manager Work?	21
Strategy for New Users	23

---

### **2 LAUNCHING TRAFFIX MANAGER FOR THE FIRST TIME**

Installing RMON Agents on Your Network	25
Launching the Traffix Manager Server	26
Launching the Traffix Manager Client	26
Stopping Traffix Manager	28
About the Main Window	28
Grouping of Objects	29
Main Window Reference	29

## **PART II HOW TRAFFIX MANAGER WORKS**

---

### **3 COLLECTING DATA**

- How Traffic Manager Processes Collected Data 35
  - RMON Overview 37
    - Remote Monitoring 37
    - RMON-2 Standard 37
  - How Traffic Manager Discovers Network Devices Using RMON-2 38
- 

### **4 GROUPING NETWORK DEVICES IN THE MAP**

- Overview 39
- Attributes 40
  - Predefined Attributes 40
- Groupings 42
  - Predefined Groupings 43
  - Creating and Assigning Attributes 44
  - Creating Groups and Ordering Attributes 45

## **PART III RUNNING TRAFFIX MANAGER**

---

### **5 LAUNCHING TRAFFIX MANAGER AFTER THE FIRST TIME**

- Launching the Traffic Manager Server 49
  - Launching a Traffic Manager Client 49
  - Client Access Levels 50
- 

### **6 CONFIGURING AGENTS FOR DATA COLLECTION**

- Supported RMON Agents and Interfaces 51
- Finding Agents for Data Collection 52
  - Configuring RMON-1 and RMON-2 Data Sources 52
  - Downloading Agent Firmware 54
  - Setting Operational Mode on 3Com Standalone RMON-2 Agents 54

---

## **7 DISPLAYING NETWORK TRAFFIC IN THE MAIN WINDOW**

- Loading Network Traffic Data 57
- Working with Objects in the Main Window 58
  - Displaying Object Information 58
  - Searching for Objects 59
  - Selecting and Deselecting Objects 59
  - Locating Objects in the Map 59
- Displaying Network Traffic Data 59
  - Displaying Connections Between Objects 60
  - Displaying Connections To and From Objects 60
  - Combining To *and* From and Between 61
  - Removing and Hiding Traffic 61
- Protocols, Applications and Favorites 61
  - Protocol Tools 62
  - User-defined Protocols 62
- Device Aggregation 64

---

## **8 DISPLAYING TRAFFIC IN GRAPHS**

- Overview 65
- Using the Graph Panel 66
- Using the Launch Graph Dialog Box 67
  - Graph Settings 69

---

## **9 USING EVENT RULES**

- Overview 71
- Predefined Event Rules 72
- Examples of Event Rules 73
  - Security Event Rules 73
  - Traffic Event Rules 74
- Configuring Event Rules 75
  - Refining Event Rules 76
- Using Event Rules 77
  - Monitoring Your Network as a Whole 77
  - Monitoring Servers 78
  - Monitoring WAN Links and Backbone Links 79
  - Implementing Business Policies 80

---

## 10 VIEWING EVENTS

- Overview 81
- Viewing Events 82
  - Filtering Events 83
  - Summarizing Events 84
  - Output of Events 84
- Viewing and Managing Selected Events 85
  - Deleting Events 85
  - Ignoring Devices or Connections 85
  - Displaying an Event in the Map 85
  - Displaying an Event in the Launch Graph Dialog Box 85
- Forwarding Events as SNMP Traps 86
  - Integrating Traction Manager SNMP Traps with HP OpenView 86

---

## 11 OVERVIEW OF REPORTING

- Overview 89
  - Types of Report 89
  - Report Instances 90
  - Output 90
  - Periods Covered by Reports 90
- Managing Reports 92
  - Creating, Editing and Deleting Reports 93
  - Scheduling Reports 94
  - Rescheduling Reports and Running Ad Hoc Reports 94
  - Managing Raw Data and Report Output 94
  - Setting Output Options 95
  - Viewing HTML Output 95
  - Monitoring Report Generation and Output 96
  - Setting the Lifetime of Raw Report Data 96
  - Setting Global Report Options 96
- Strategy for Reporting 97
  - Getting Started 97
  - How Long Does it Take to Generate Reports? 97
  - Tips and Hints 97
- Effects of Grouping on Reports 98

---

## **12 REPORT TYPES**

Report Templates	99
Activity Reports	99
Top N Reports	99
Connection Activity Report	100
Device Activity Report	101
Group Activity Report	102
Segment Activity Report	103
Top N Connections Report	105
Top N Devices Report	107
Top N Groups Report	109
Top N Segments Report	110

## **PART IV APPENDICES AND INDEX**

---

### **A TROUBLESHOOTING TRAFFIX MANAGER**

Troubleshooting Traffic Manager	115
Troubleshooting Reports	116
Diagnosing Reporting Problems	116

---

### **B DATABASE MANAGEMENT USING TRAFFIX CONTROL PANEL**

Overview of Traffic Control Panel	121
Overview of Database Applications	122
Database Setup	122
Database Maintenance	123
Subnets Editor	125
Attribute Lookup	125
DHCP Setup	125
Startup Options	125
Default DNS Domain	126
Upgrading Traffic Manager 2.0	126
Before Deinstalling	126
Deinstalling Traffic Manager 2.0	127
Program Groups and Start Menu Entries	127

---

## **C AGGREGATING DEVICES**

- Overview 129
- Default Aggregation 129
  - Specifying an Aggregation Policy 130

---

## **D USING THE SUBNETSDB FILE**

- Using the SubnetsDB File 133
  - How Subnet Grouping Works 135

---

## **E AUTOMATIC ATTRIBUTE ASSIGNMENT**

- Overview 137
- Contents of the User-defined Attributes Configuration File 138
  - File Format 139
- Performing Attribute Assignment 140
- Using the fileattrs Program 140
  - Configuration File Format 140
  - Running fileattrs 141
  - How fileattrs Works 141
- Using the dblookup Program 142
  - Lookup Database Structure 142
  - Default Values 143
  - Access Database 143
  - Excel Worksheet 144
  - Excel Workbook 144
  - Running dblookup 144
  - How dblookup Works 144
- Writing your own program 145
  - Structure of an Attribute Lookup Program 145
  - Writing and Building Your Own Attribute Lookup Program 147
  - Testing Attribute Lookup Programs 149

---

## **F SUPPORTED RMON-2 DEVICES**

- 3Com Agents 151
- Supported Interface Types 151



---

## **G CONFIGURING 3COM STANDALONE RMON-2 AGENTS**

Downloading Firmware to 3Com Standalone Agents 153

Setting the Operational Mode on 3Com Standalone RMON-2 Agents 154

---

## **H DHCP**

How Traffix Manager Monitors DHCP Devices 157

What Effect Do DHCP Devices Have On The Map? 157

---

## **I USING RMON-1 AGENTS**

Monitoring Network Segments Using RMON-1 Agents 159

---

## **J RMON AND SNMP TABLES RETRIEVAL**

SNMP Tables used by Traffix Manager 161

---

## **K TECHNICAL SUPPORT**

Online Technical Services 163

World Wide Web Site 163

3Com Knowledgebase Web Services 163

3Com FTP Site 164

3Com Bulletin Board Service 164

3Com Facts Automated Fax Service 165

Support from Your Network Supplier 165

Support from 3Com 165

Returning Products for Repair 167

---

## **GLOSSARY**

---

## **INDEX**

---

## **3COM CORPORATION LIMITED WARRANTY**



# ABOUT THIS GUIDE

This guide describes Transcend® Traffix™ Manager version 3.0 for Windows NT. This application gathers, displays and analyzes enterprise-wide network traffic.

Procedural information on how to perform all tasks using Traffix Manager, as well as context-sensitive information about each dialog box, is provided in the online help.

This guide is intended for network administrators. It assumes a working knowledge of local area network (LAN) operations.



*If the information in the release notes shipped with this product differs from the information in this guide, follow the instructions in the release notes.*

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

<http://support.3com.com/infodeli/tools/netmgt/>

---

## How To Use The Traffix Manager Documentation

[Table 1](#) shows where to find information in the Traffix Manager User Guide and Online Help.

**Table 1** Where to find specific information

If you are looking for	Turn to
An overview of Traffix Manager, describing the main features of the application and how it works, and providing a strategy for new users to get started with the application.	<a href="#">Chapter 1</a>
Procedures for launching Traffix Manager the first time you use it.	<a href="#">Chapter 2</a>
A description of all menu options in the main window.	<a href="#">Chapter 2</a>

(continued)

**Table 1** Where to find specific information (continued)

If you are looking for	Turn to
An overview of the RMON-1 and RMON-2 standards, and an introduction to how Traffic Manager uses RMON-2 agents to collect data from your network.	<a href="#">Chapter 3</a>
Information on grouping devices to create views of your network in the Map.	<a href="#">Chapter 4</a>
Procedures for launching Traffic Manager <i>after</i> the first time.	<a href="#">Chapter 5</a>
Information on configuring RMON-1 and RMON-2 agents to collect network traffic data.	<a href="#">Chapter 6</a>
A guide to working with objects in the main window and to finding and selecting objects in the Map and Object List.	<a href="#">Chapter 7</a>
Information on focusing the views of your network in the Map by filtering the protocols displayed.	<a href="#">Chapter 7</a>
Information on setting up user-defined protocols on compatible agents.	<a href="#">Chapter 7</a>
Information on displaying network traffic in graphs and manipulating the graph display.	<a href="#">Chapter 8</a>
Information on setting up rules to trigger events when the traffic on your network changes.	<a href="#">Chapter 9</a>
Information on viewing events in the Event List, in the Map and in graphs.	<a href="#">Chapter 10</a>
A description of Traffic Manager's reporting tools, information on creating and scheduling reports and a reporting strategy for new users.	<a href="#">Chapter 11</a>
A description of the different types of report produced by Traffic Manager and a guide to interpreting the charts in generated reports.	<a href="#">Chapter 12</a>
Procedures for troubleshooting Traffic Manager process and agent problems.	<a href="#">Appendix A</a>
Procedures for troubleshooting reporting problems.	<a href="#">Appendix A</a>
Procedures for managing the Traffic Manager database using the Traffic Control Panel.	<a href="#">Appendix B</a>
Procedures for aggregating traffic and filtering data.	<a href="#">Appendix C</a>
Information on grouping the devices on your network by subnet.	<a href="#">Appendix D</a>
Procedures for setting up automatic assignment of attributes to network devices, including examples of user programs.	<a href="#">Appendix E</a>
A list of the RMON-2 interface types supported by Traffic Manager.	<a href="#">Appendix F</a>
Procedures for downloading firmware to standalone agents.	<a href="#">Appendix G</a>
Procedures for setting the operational mode on 3Com standalone RMON-2 agents.	<a href="#">Appendix G</a>
Information on using the TFTP server.	<a href="#">Appendix G</a>
Information on the effect DHCP devices have on the Map.	<a href="#">Appendix H</a>
Information on monitoring segments of your network using RMON-1 only.	<a href="#">Appendix I</a>
A list of the RMON tables which are retrieved by Traffic Manager.	<a href="#">Appendix J</a>
3Com technical support information.	<a href="#">Appendix K</a>
Detailed procedural information on how to perform all tasks using Traffic Manager.	Online Help
Context-sensitive information about each application dialog box, describing functions and fields.	Online Help

(continued)



**Table 1** Where to find specific information (continued)

If you are looking for	Turn to
Information about what's new in this release of Traffic Manager.	Release Notes
A list of known problems in this release of Traffic Manager.	Release Notes

## Conventions

[Table 2](#) and [Table 3](#) list conventions that are used throughout this guide.

**Table 2** Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device

**Table 3** Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Syntax	The word "syntax" means that you must evaluate the syntax provided and then supply the appropriate values for the placeholders that appear in angle brackets. Example:  To enable RIPIP, use the following syntax:  <code>SETDefault !&lt;port&gt; -RIPIP CONTrol = Listen</code>  In this example, you must supply a port number for <port>.
<b>Commands</b>	The word "command" means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example:  To remove the IP address, enter the following command:  <code><b>SETDefault !0 -IP NETaddr = 0.0.0.0</b></code>
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example:  Press Ctrl+Alt+Del

(continued)

**Table 3** Text Conventions (continued)

Convention	Description
Words in <i>italics</i>	<p>Italics are used to:</p> <ul style="list-style-type: none"> <li>■ Emphasize a point.</li> <li>■ Denote a new term at the place where it is defined in the text.</li> <li>■ Identify menu names, menu commands, and software button names. Examples:</li> </ul> <p>From the <i>Help</i> menu, select <i>Contents</i>.</p> <p>Click <i>OK</i>.</p>

---

## Terminology Used in this Guide

Refer to the [Glossary](#) at the end of this User Guide for definitions of terms. Terms which are defined in the Glossary are italicized at their first use in the User Guide.

---

## Related Documentation

The following documents and Web sites contain useful networking information.

### Documents

- Transcend Traffix Manager Release Notes and Installation Instructions
- 3Com Firmware documentation
- Transcend Traffix Manager Database Schema at <http://support.3com.com/infodeli/tools/netmgt/traffix/family.htm>
- Transcend Management Software Network Troubleshooting Guide at <http://support.3com.com/infodeli/tools/netmgt/tncsunix/family.htm>

### Web Sites

#### **RMON-1/RMON-2**

RMON-1 and RMON-2 Backgrounder:

<http://www.3com.com/nsc/501305.html>

RMON-1 Request for Comment:

<http://www.it.kth.se/docs/rfc/rfcs/rfc1757.txt>

RMON-2 Request for Comment:

<http://www.it.kth.se/docs/rfc/rfcs/rfc2021.txt>

RMON-2 Protocol Identifiers:

<http://www.it.kth.se/docs/rfc/rfcs/rfc2074.txt>

### Miscellaneous

List of third-party agents which are supported by Traffic Manager:

[http://www.3com.com/network\\_management/probe\\_interop](http://www.3com.com/network_management/probe_interop)

Links to network management information:

<http://snmp.cs.utwente.nl>

Internet Engineering Task Force home page:

<http://www.ietf.cnri.reston.va.us>

Network Management Resource Database:

<http://www.cforc.com/cwk/net-manage.cgi>

---

## Documentation Comments

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

**[pddtechpubs\\_comments@3com.com](mailto:pddtechpubs_comments@3com.com)**

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- Traffic Manager 3.0 User Guide
- Part Number 09-1825-000
- Page 25



*Do not use this e-mail address for technical support questions. For information about contacting 3Com technical support, see [Appendix K](#).*

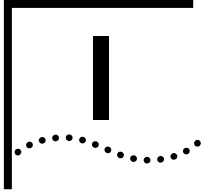
---

## **Year 2000 Compliance**

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 Web page:

**<http://www.3com.com/products/yr2000.html>**

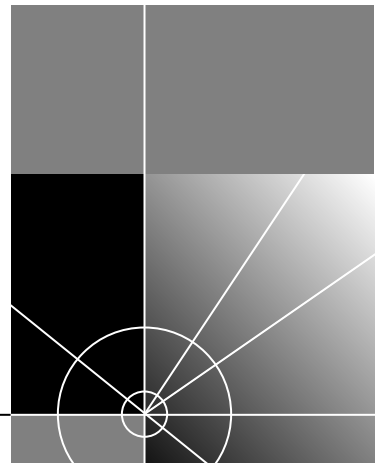




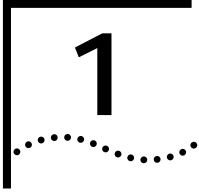
# GETTING STARTED WITH TRAFFIX MANAGER

[Chapter 1](#) [Traffix Manager Overview](#)

[Chapter 2](#) [Launching Traffix Manager for the First Time](#)







# TRAFFIX MANAGER OVERVIEW

This chapter introduces you to Trafix™ Manager.

It contains the following sections:

- [What to Read First](#)
- [Features of Trafix Manager](#)
- [How Does Trafix Manager Work?](#)
- [Strategy for New Users](#)

---

## What to Read First

Chapters 1–5 contain a conceptual overview of the processes you need to follow in order to get to the stage where Trafix Manager is displaying network traffic data for analysis. Read these chapters to understand:

- How Trafix Manager can facilitate network monitoring and administration.
- How to start using Trafix Manager.
- How to launch Trafix Manager, for the first time and subsequently.
- What you will see displayed in the main window when you launch Trafix Manager.
- How Trafix Manager works and how to use it to collect data from your network.

From Chapter 6 onwards, the guide contains concepts for tailoring Trafix Manager to the requirements of your own network.

The appendices at the end of the guide contain troubleshooting information, reference information and instructions for tasks you only need to perform occasionally.

The Traffic Manager online help contains detailed procedural information on how to perform all tasks, and information about each application dialog box.

The Traffic Manager Release Notes contain installation information, and a list of known problems with this release.

---

## Features of Traffic Manager

Traffic Manager collects and displays information about the application traffic on your network, allowing you to understand who is using your network, and how it is being used. This helps you move from reacting to changes in network traffic to anticipating the ways that applications use the network.

Traffic Manager provides the following features for network monitoring:

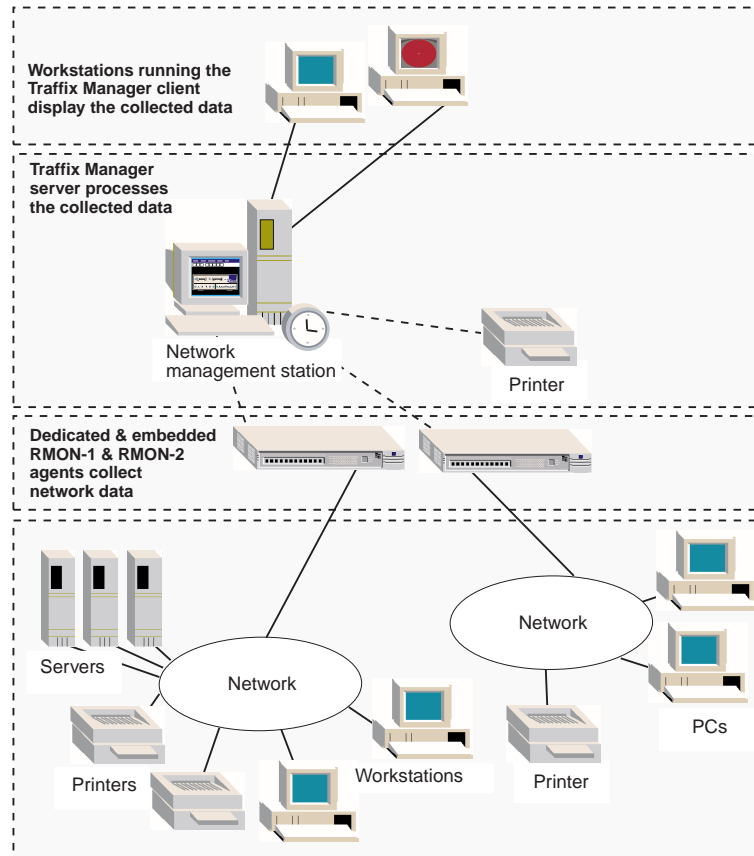
- **Graphical display of network traffic** — The graphical display of traffic patterns shows how applications are being used on your network. Traffic Manager begins with a high-level, logical view of network traffic to show overall connections between groups of devices. You can then zoom in to see more detailed information about conversations, servers and other devices on the network. You can access historical information to help you make informed decisions regarding resource utilization, capacity planning and network growth.
- **Generation of traffic events** — Once data collection from your network has begun, you can build up a picture of typical network usage. You can then specify rules to monitor unusual events on your network, such as unauthorized access or devices which are using an abnormal amount of bandwidth. When these rules are triggered, Traffic Manager generates events. This is especially useful if you do not have time to monitor the network continuously but want to view a log of the events generated over a specified period.
- **Fully automated reporting tools** — The reporting tools allow you to generate color reports automatically to provide information about your network. For example, you can create reports on the busiest segments and devices, or on web usage. Traffic Manager reports can be produced in HTML format and viewed through a web browser, as well as professional printed color reports and CSV files for other tools such as Microsoft Excel.
- **Client/server architecture** — You can run multiple and remote clients against a single server.

- **Industry standards** — Traffic Manager supports the IETF RMON-2 standard, which enables information about *network* and *application layer* protocol communication patterns to be collected. See [“RMON Overview”](#) on [page 37](#) for more information.
- **Open Database for Storage** — Traffic Manager has a relational database as its core data repository, enabling easy management of large quantities of data collected from several monitoring points.

---

## How Does Traffic Manager Work?

Traffic Manager is a client/server application. The Traffic Manager server periodically polls RMON-1 and RMON-2 agents on your network for data about conversations between devices. See [“RMON Overview”](#) on [page 37](#) for more information about RMON-1 and RMON-2 agents.

**Figure 1** Traffic Manager Gathers Data from the Network

The collected data is stored in the database, and checked against configured event rules to see whether a traffic event should be generated. See [Chapter 9, "Using Event Rules"](#), for more information.

The Traffic Manager client is used to view the collected data, or to configure the operation of the Traffic Manager server. The collected data can be viewed as traffic conversations on the Map, in various charts, or in one of the various reports. See ["About the Main Window"](#) on [page 28](#) for more information about the Map.

---

## Strategy for New Users

If you have just begun using Traffix Manager to monitor your network, you should do the following:

- Set up a limited number of agents from which to collect data until you become familiar with the data collection process. Then you can configure other agents on your network. See [“Configuring RMON-1 and RMON-2 Data Sources”](#) on [page 52](#) for more information.
- Collect and monitor data for a few days until you have learned about:
  - The normal traffic levels and rates on your network.
  - The number of devices on your network and other devices being communicated with, for example World Wide Web (WWW) sites.

Over a few weeks you can regularly view Traffix Manager reports to get a feel for the normal and peak traffic rates on your network. At that point you can:

- Specify rules defined by your use of Traffix Manager, to generate exception events. See [Chapter 9, “Using Event Rules”](#) for more information.
- Combine groups of low priority devices on your network; for example, combining all WWW sites into a single group to reduce the number of devices Traffix Manager has to track. See [“Device Aggregation”](#) on [page 64](#) for more information.



*Keep the Traffix Manager server running at all times so that data is continuously stored and prepared for reporting. The client does not need to be kept running. See [“Stopping Traffix Manager”](#) on [page 28](#).*





# 2

## LAUNCHING TRAFFIX MANAGER FOR THE FIRST TIME

This chapter provides information on launching Traffix™ Manager for the first time. Information on installing Traffix Manager is documented in the Release Notes which are shipped with this product.

It contains the following sections:

- [Installing RMON Agents on Your Network](#)
- [Launching the Traffix Manager Server](#)
- [Launching the Traffix Manager Client](#)
- [Stopping Traffix Manager](#)
- [About the Main Window](#)
- [Main Window Reference](#)

---

### Installing RMON Agents on Your Network

Before you can launch Traffix Manager, you need to have at least one RMON agent installed on your network to collect traffic data. See Chapter 8 of the Transcend® NCS Network Administration Guide for information on how to deploy RMON agents on your network. The TNCS Network Administration Guide is available from the 3Com web site:

**`http://support.3com.com/infodeli/tools/netmgt/tncsunix/family.htm`**

Refer to the Firmware Upgrade documentation for information on downloading firmware to RMON agents. The latest version of the Firmware Upgrade documentation is available from the 3Com web site:

**`http://www.support.3com.com/infodeli/tools/netmgt/rmonprob/family.htm`**

---

## Launching the Traffic Manager Server

There are two steps to launching Traffic Manager: you must launch the Traffic Manager server first and then launch the Traffic Manager client.

To launch the Traffic Manager server:

- 1 Select *Programs* from the *Start* menu, and open the directory in which you installed the Traffic Control Panel. The default path is:  
*Start>Programs>Transcend Traffic Manager>Transcend Traffic Manager v3.0 Control Panel*.
- 2 Click *Database Setup* to launch the Database Setup dialog box.
- 3 Click *Create New Database* to create an empty Traffic Manager 3.0 database.
- 4 You can change the database size from the Database Maintenance dialog box. Click *Database Maintenance* in the Traffic Control Panel to open the Database Maintenance dialog box.
- 5 Start the Traffic Manager server by clicking *Start Server* in the Traffic Control Panel.

---

## Launching the Traffic Manager Client

To launch the Traffic Manager client, select *Programs* from the *Start* menu, and open the directory in which you installed the client. The default path is *Start>Programs>Transcend Traffic Manager>Transcend Traffic Manager v3.0 Client*.

The first time that you start the Traffic Manager client after installation, you will be automatically logged in as the Traffic Manager Administrator to give you the rights to configure Traffic Manager. See "[Client Access Levels](#)" on [page 50](#) for more information on administrator and read-only user access.

When the client is first started, it tries to locate the Traffic Manager server through the use of a broadcast message. If the system on which the client is running is not in the same broadcast domain as the server, this broadcast message will fail, and the client will not be able to connect to the server. In order to solve this problem, you may tell the client explicitly where the server is. See "Running the Client in a Different Broadcast Domain to the Server" on page 24 of the Traffic Manager Release Notes for more information.

After you have started the Traffic Manager client for the first time, the startup wizard appears automatically. This will guide you through the

configuration of data sources, and take you to the point where traffic data is displayed in the main window.

The startup wizard first prompts you for the *DNS domain(s)* of those devices which you want to monitor in detail. Traffic Manager considers this specified DNS domain to be your “local network”. The wizard automatically defaults to specify the domain in which the management station is running, but you can make your own selection.

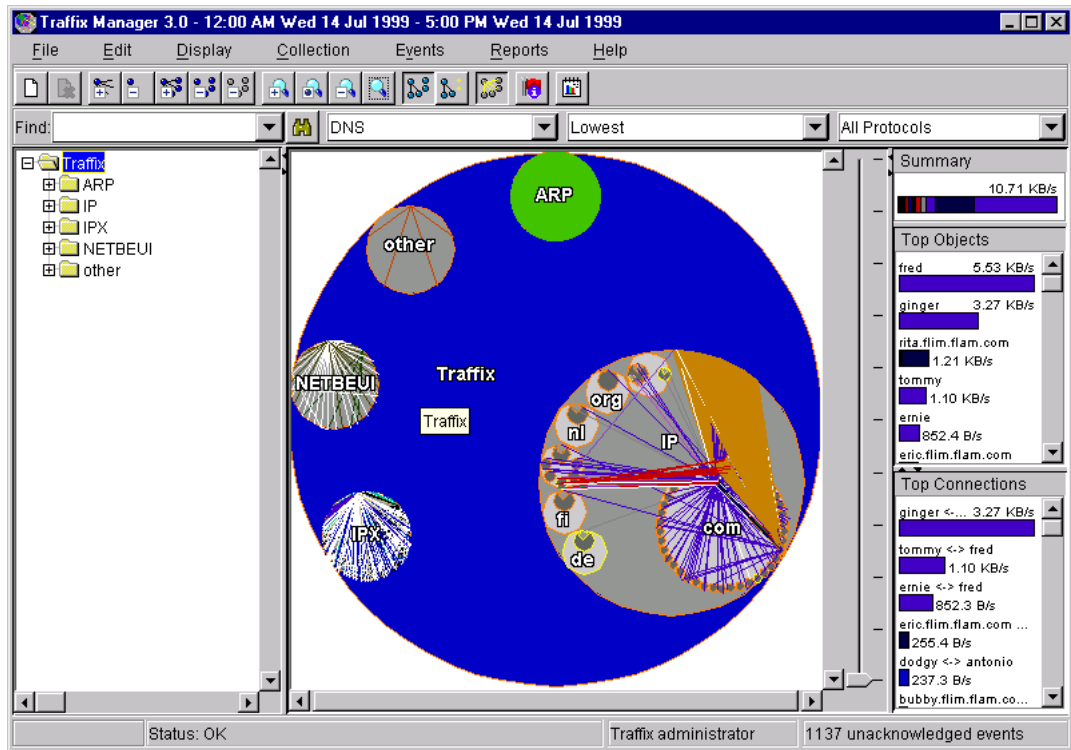
This concept of what constitutes your local network affects the event rules and aggregation functionality in the following ways:

- The event rules which are predefined by Traffic Manager use the local network as the default group. See [Chapter 9, “Using Event Rules”](#) for more information.
- When you choose to aggregate devices on your network, by default any devices within your local network will be kept in detail and not aggregated. See [Appendix C, “Aggregating Devices”](#) for more information.

Once you have specified your local network, the startup wizard automatically finds RMON-2 agents within a given range of addresses, or uses the subnet address of the management station. See [“RMON Overview”](#) on [page 37](#) for more information. Traffic Manager uses the agents found, and/or those added manually by you, and starts to collect data.

The normal polling interval for data is every 30 minutes, but the first time Traffic Manager does a quick poll of your network in approximately five to ten minutes to make data available for display and monitoring as soon as possible. The wizard displays feedback as the first poll progresses. When the first poll is complete, the Map is displayed in the main window, showing the traffic conversations seen on your network.

Figure 2 Traffic Manager Main Window



## Stopping Traffic Manager

To stop a Traffic Manager client, click *Exit* on the *File* menu in the main window.

To stop the Traffic Manager server, click *Stop Server* in the Traffic Control Panel. Stopping the server will exit all clients.

## About the Main Window

In the main window of Traffic Manager, you can view both a tree and a graphical representation of the objects (devices and groups of devices) in your network, and the traffic between them.

The main window is divided into three main parts:

- **Object List** — Contains a hierarchical tree of the objects seen on your network.

- **Map** — Contains a graphical representation of the network, showing the hierarchy of objects and the traffic flowing between them.
- **Graph Panel** — Shows the most significant network activity of the currently selected objects in graphical form. See [Chapter 8, “Displaying Traffic in Graphs”](#), for further information about graphing.

### Grouping of Objects

Within the Object List and the Map, objects are grouped in a hierarchy. By default, objects are grouped according to their DNS attributes.

You can easily change the way objects are grouped. See [Chapter 4, “Grouping Network Devices in the Map”](#) for further information about grouping devices.

To expand a group in the Object List and view its contents, click the plus sign (+) next to a group. Traffix Manager automatically expands the hierarchy of objects in the Object List only. To collapse a group, click the minus sign (–) next to the group.

---

## Main Window Reference

This section contains a quick reference guide to the menu options in the main window.

**Table 4** Traffix Manager Main Window Menu Options

Menu	Option	Function
<b>File</b>	Load Traffic...	Launches the Load Traffic dialog box from which you can specify a time range of data to load into the client.
	User Authorization...	Launches the User Authorization dialog box which displays all users who have a client running. Also allows you to change between Traffix administrator and read-only user.
	Print...	Launches the standard Printer Options dialog box from which you can output the contents of the main window to a printer or file.
	Exit	Exits the Traffix Manager client.
<b>Edit</b>	Find...	Launches the Find Object dialog box from which you search for objects in the Object List.
	Attributes...	Launches the Attribute dialog box from which you add device attributes and assign attribute values to the selected devices.

(continued)

**Table 4** Traffix Manager Main Window Menu Options (continued)

Menu	Option	Function
	Groupings...	Launches the Groupings dialog box from which you can create, modify and delete groupings from this dialog box.
	Reload Attributes	Launches the Reload Attributes dialog box from which you reload attributes for devices in the Map.
<b>Display</b>	Add Connections To and From	Adds all traffic connections going to and from the selected objects to any other objects on the network within the loaded time range. Use to determine which groups or devices the selected objects are talking to. Traffic must be loaded first.
	Remove Connections To and From	Removes all traffic for selected objects on the Map.
	Add Connections Between	Adds traffic connections going between the selected objects only. Use to: <ul style="list-style-type: none"> <li>■ Map connections between specific devices</li> <li>■ Map connections within and between specific groups.</li> </ul> Traffic must be loaded first.
	Remove Connections Between	Removes traffic connections between selected objects on the Map.
	Remove All Connections	Removes all traffic connections on the Map, regardless of what is selected.
	Show Mapped Connections	Toggle. Shows or hides connections on the Map. Use to view groupings which are hidden by connection lines. If connections are shown, a tick appears next to this option on the menu and the toolbar button is depressed.
	Map All Objects	Displays all loaded objects in the Map. Selected by default.
	Map Connected Objects	Displays only those devices that have a connection showing in the Map.
	Labels...	Launches a sub-menu in which you specify which label (Name/Network Address/MAC Address) to use for devices in the Map and Object List.
	Protocols...	Launches the Protocols dialog box from which you select and edit the protocols to be displayed in the Map, and save favorite protocol selections.

(continued)

**Table 4** Traffix Manager Main Window Menu Options (continued)

Menu	Option	Function
	Zoom...	<p>Launches a sub-menu in which you select from the following:</p> <ul style="list-style-type: none"> <li>■ <b>Zoom In</b> — Zooms into area containing currently selected objects. If no objects are selected, the currently displayed area is magnified.</li> <li>■ <b>Zoom To</b> — Zooms to selected objects, magnifying them in the Map as much as possible.</li> <li>■ <b>Zoom Out</b> — Zooms out of area containing currently selected objects. If no objects are selected, zooms out of the currently displayed area.</li> <li>■ <b>Reset Zoom</b> — Zooms out to fit window so that the whole <i>Traffix</i> group can be seen.</li> </ul>
	Graph Panel Settings...	Launches the Graph Panel Settings dialog box for configuring the graph panel of the main window.
	Launch Graph	Launches the Launch Graph dialog box. Allows you to view graphs for the object(s) selected in the Map.
<b>Collection</b>	Configure Agents...	Launches the Configure Agents dialog box from which you configure agents to collect data from your network.
	Agent Hardware Maintenance...	Launches the Agent Hardware Maintenance dialog box from which you can download firmware to agents, change the mode of agents and reboot agents.
	Aggregation...	Launches the Aggregation dialog box from which you can specify the aggregation policy.
	Database Size...	Launches the Database Size dialog box, which shows how much disk space the database is using.
<b>Events</b>	Event Rules...	Launches the Event Rules dialog box from which you can add, edit and enable/disable event rules.
	Show Rules for Current Selection...	Launches a dialog box showing which event rules apply to the selected object.
	Event List (All)...	Launches the Event List showing all events that have been generated, which have not yet been acknowledged.
	Event List (Current Selection)...	Launches the Event List showing all events that have been generated for the selected object, including events that have been acknowledged
<b>Reports</b>	Report Manager...	Launches the Report Manager from which you create, modify and delete reports. You also schedule report output, set global report options and manage the reporting process from this dialog box.
<b>Help</b>	Contents	Launches online help with the Contents tab selected.

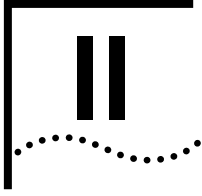
(continued)

**Table 4** Traffix Manager Main Window Menu Options (continued)

Menu	Option	Function
	Index	Launches online help with the Index tab selected.
	About	Launches the About Traffix Manager screen, giving the version name and numbers of the application.

See [Chapter 7, “Displaying Network Traffic in the Main Window”](#) for detailed information on working with objects in the main window.

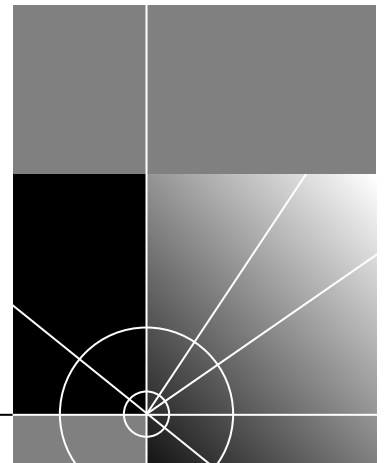




# HOW TRAFFIX MANAGER WORKS

[Chapter 3](#) [Collecting Data](#)

[Chapter 4](#) [Grouping Network Devices in the Map](#)





# 3



## COLLECTING DATA

This chapter describes how Trafficx™ Manager collects data from your network.

It contains the following sections:

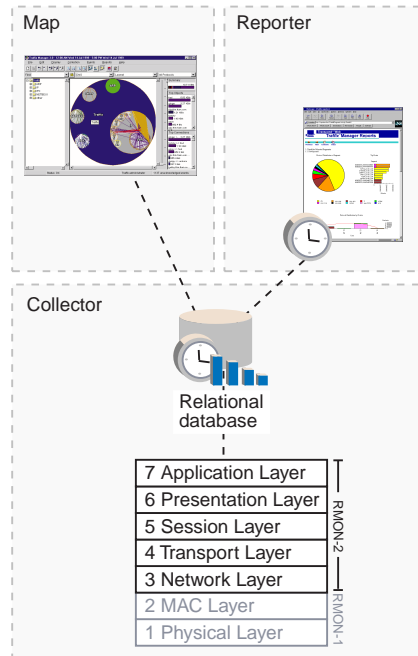
- [How Traffic Manager Processes Collected Data](#)
- [RMON Overview](#)
- [How Traffic Manager Discovers Network Devices Using RMON-2](#)

---

### How Traffic Manager Processes Collected Data

Traffic Manager collects and correlates data from stand-alone and embedded *RMON-1* and *RMON-2* agents, from both 3Com and other vendors. This data provides a complete picture of enterprise network traffic for performance management and trend analysis.

At scheduled intervals, Traffic Manager's Collector process uploads the collected traffic data, processes the contents and stores the results in a relational database.

**Figure 3** Collected Data is added to a Relational Database

From the collected data, you can build up a picture of normal levels of network traffic and typical network usage. You can then configure event rules which provide you with information about the traffic on your network and network security. When these rules are exceeded, Traffic Manager generates events which can be viewed in the Map or in graphs. See [Chapter 9, “Using Event Rules”](#) for more information about configuring events, and [Chapter 8, “Displaying Traffic in Graphs”](#).

The contents of the relational database can be retrieved by the Map and Reporter processes. The Map retrieves data for a given period and displays it graphically. You can manipulate the display, grouping network devices and filtering traffic, to view your network in any way you want. See [Chapter 4, “Grouping Network Devices in the Map”](#) for more information.

The Reporter uses the same data to generate scheduled reports, which can then be distributed as HTML files for viewing by a web browser or to your printer. See [Chapter 11, “Overview of Reporting”](#) for more information.

---

## RMON Overview

Traffic Manager supports all agents that are compliant with the Internet Engineering Task Force (IETF) Remote MONitoring Management Information Base Version 1 (RMON-1 MIB), defined in RFC 1757, and Version 2 (RMON-2 MIB), defined in RFCs 2021 and 2074.

The RMON standards bring the following advantages to network monitoring:

- They provide an effective and efficient way to monitor the behavior of the entire LAN.
- They distribute the load of network monitoring between both remote devices and management stations.
- They are widely-used standards.

An RMON agent can be deployed as a stand-alone probe or embedded within another device. Management applications communicate with RMON agents using the *SNMP protocol*. In this way, RMON agents collect information about network behavior, and can then transfer it on command to an analysis site.

RMON agents have the following benefits:

- They improve the efficiency of staff by allowing them to remain in a centralized site while collecting information from widely dispersed LAN segments.
- They can continuously monitor and collect information and deliver it before problems occur, allowing you to take a proactive approach to managing your network.
- Each remote agent can handle requests from multiple management stations.

## Remote Monitoring

A client sets RMON variables on the device to specify measurement intervals, monitored thresholds and other operational parameters. The remote device collects and stores information and delivers it to a client on request.

## RMON-2 Standard

RMON-2 is an extension of the RMON-1 standard. The most visible and most beneficial capability of RMON-2 is monitoring above the MAC layer. RMON-2 collects statistics at the network and application layers of the protocol stack to provide a view of the whole network rather than a

single segment. Traffic Manager uses RMON-2 functionality to build up a picture of communicating devices on the network and the traffic flowing between them, including network layer addresses and protocols seen.



*For further information on RMON-1 and RMON-2, refer to the 3Com® RMON-1 and RMON-2 Backgrounder on the 3Com Web Site:*

**<http://www.3com.com/nsc/501305.html>**.

---

### How Traffic Manager Discovers Network Devices Using RMON-2

An agent which supports RMON-2 is able to watch the packets on the network segment to which it is attached. Depending on the protocol in use, most packets typically contain a source and destination address. The RMON-2 agent decodes this address information and uses it to build tables of data about the communicating devices and the traffic flowing between them, including network layer addresses and protocols seen. This information is then retrieved by Traffic Manager and is used to build a graphical topology of your network (the Traffic Manager Map) and to compile a list of active devices on your network.

As a result of the RMON-2 method of discovering devices, you may see more than one object corresponding to the same physical device. For example, separate entries for a device may be made under its ARP, IP and IPX addresses. For the same reason, “non-device” objects, such as IP broadcast and multicast addresses, will appear in the Map.



*With no RMON-2 conversation data collected, Traffic Manager is able to perform only limited functions.*

*If an agent selected for data collection supports RMON-1 only, Traffic Manager is only able to collect line statistics data from that agent and perform basic agent maintenance operations. See [Appendix I, “Using RMON-1 Agents”](#) for more information.*

# 4

## GROUPING NETWORK DEVICES IN THE MAP

This chapter contains the following sections:

- [Overview](#)
- [Attributes](#)
- [Groupings](#)

---

### Overview

With Traffix™ Manager, you can group devices in the Map according to your own criteria. You can view the use of your network by, for example, cost center, business unit, workgroup, business-critical connection or geographical location.

You can then filter the display of traffic data further by selecting which protocols to display. You can then view traffic connections using these specified protocols only.

When used with the reporting tools in Traffix Manager, you can monitor and document the use of the network by selected groups and distribute this information as and where needed. See [Chapter 11, “Overview of Reporting”](#) for further information.

Using the events functionality in Traffix Manager, you can monitor your network traffic and the security of your network. You can select protocols or devices to monitor in this way. See [Chapter 9, “Using Event Rules”](#) for more information.

## Attributes

To understand how Traffix Manager groups devices in the Map, it helps to be familiar with the concepts of *attributes* and *groupings*.

An *attribute* is a label for a piece of information about a device: for example, location or *IP address*. Traffix Manager has a number of predefined attributes; you can change these or add your own.

At any one time, each attribute of a particular device is either currently unassigned (not defined), or has a single value. For example, the value of the location of a device might be *Boston*, or the location might be unknown, or *unassigned*.

## Predefined Attributes

There are a number of predefined attributes in Traffix Manager that you can use to create your own groupings. For these predefined attributes, values are usually assigned automatically as each device is discovered.

You cannot delete a predefined attribute, or change its name.

**Table 5** Predefined Attributes

Name	Description
Name	DNS Name or Network Layer address.
NL Type	Network Layer protocol.
NL Addr	Network Layer (IP) address.
Network	Protocol-specific network number, generated from the Network Layer address.
Subnet	This attribute is set to SubnetsDB if the object matches an entry in the SubnetsDB file. Otherwise it is unassigned. See <a href="#">Appendix D, "Using the SubnetsDB File"</a> .
Discovery Time	Time (in seconds, since January 1st 1970) when Traffix Manager discovered device.
Last Activity Time	Time (in seconds, since January 1st 1970) when the device last sent or received traffic.
Type	Device/Aggregated/DHCP Device.

(continued)



**Table 5** Predefined Attributes (continued)

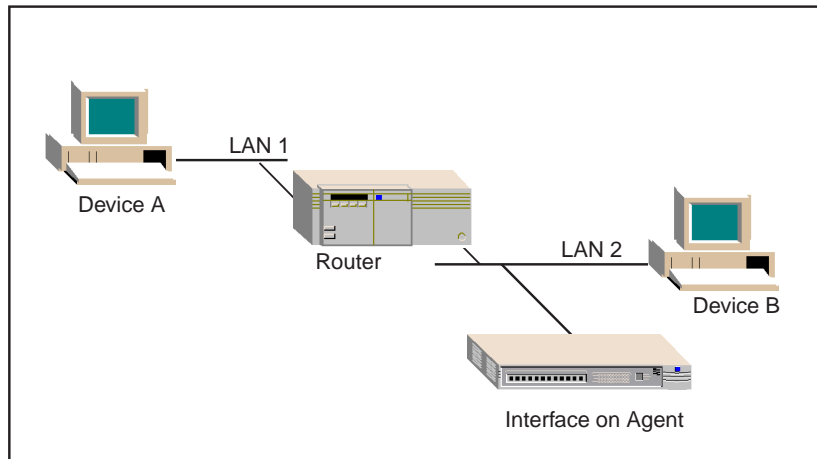
Name	Description
MAC Addr	Only devices which are in the same broadcast domain as the interface on an RMON-2 agent will have the MAC address attribute assigned to them. See <a href="#">“Assigning MAC Addresses”</a> on <a href="#">page 42</a> for an example of this.
Vendor	<p>The Vendor attribute is only assigned if the following criteria are met:</p> <ul style="list-style-type: none"> <li>■ The MAC Address attribute is assigned (see above).</li> <li>■ The MAC address matches a vendor prefix in the <code>vendor.map</code> file: <pre data-bbox="758 696 1058 777">&lt;installdir&gt;/ TraffixServer/config/ vendor.map</pre> </li> </ul>
DNS Layer 1	The top level of the DNS naming scheme (for example, <i>com</i> ).
DNS Layer 2, DNS Layer 3,... DNS Layer 8	<p>Lower levels of the DNS naming scheme.</p> <p>Non-IP devices do not have DNS Layer attributes assigned. IP devices will only have DNS Layer attributes assigned if the following criteria are met:</p> <ul style="list-style-type: none"> <li>■ Domain Name System (DNS) is implemented at your site.</li> <li>■ DNS name <code>lookup</code> is enabled on the system where the server is running and the name <code>lookup</code> succeeds.</li> </ul> <p>See <a href="#">“Default DNS Domain”</a> on <a href="#">page 126</a> for information on assigning a default DNS domain to devices.</p>

## Assigning MAC Addresses

When the client is first started, it tries to locate the Traffix Manager server through the use of a broadcast message. If the system on which the client is running is not in the same broadcast domain as the server, this broadcast message will fail, and the client will not be able to connect to the server. In order to solve this problem, you may tell the client explicitly where the server is. See “Running the Client in a Different Broadcast Domain to the Server” on page 24 of the Traffix Manager Release Notes for more information.

[Figure 4](#) shows two LANs linked by a router.

**Figure 4** Observed Network Devices



If Device A communicates with Device B, the agent interface on LAN2 records an entry for both devices and both devices appear in the database. However, although Device B has a MAC address associated with it in the database, Device A does not. Because the conversation is taking place across a router, Traffix Manager is not able to associate Device A with the MAC address of the router.

---

## Groupings

A *grouping* is a named, ordered list of attributes. For example, a grouping named *Geographical* might have the first attribute *Country*, and second attribute *City*. Traffix Manager is supplied with predefined groupings; you can change these or add your own. Before proceeding, spend some time working out how you want to group devices on your network.

The Map shows a hierarchical view of the devices in your network according to the selected grouping. By selecting a *Geographical* grouping for example, devices will be grouped according to which country they are in. Within each country, devices may be grouped according to which city they are in.

The hierarchy of groups in the Map corresponds to the order of attributes in the selected grouping. Devices with the same value for the first attribute, such as *Germany* for example, are grouped together. Within each country group, devices with the same value for the second attribute, such as *Munich*, are grouped together. You can further refine the hierarchy by adding attributes to the grouping: a third attribute *Department1*, for example.

If a device does not have a value assigned to it for an attribute, then this device may appear in a group called *unassigned*. The unassigned group is known as a redundant group. You can collapse redundant groups, so that devices within them appear in a higher-level (assigned) group instead.

## Predefined Groupings

There are four predefined groupings in Traffix Manager:

- **DNS** — Devices are grouped according to their DNS name.

This grouping is made up of the predefined attributes Network Layer Type (for example, IP, IPX, DECNet, ATALK), and DNS Layer 1 through DNS Layer 8. See [Table 5](#) for more information about these attributes.

- **Type and Network** — Devices are grouped by their Network Layer Type and network address.

This grouping is made up of the predefined attributes *NL Type* and *Network*. All devices in the Map have both of these attributes assigned so there are no redundant groups. See [Table 5](#) for more information about these attributes.

Within this grouping, devices are grouped by their major protocol classes, that is, their NL Type, and are then further grouped in a way appropriate to each protocol. For example, DECNet devices are grouped by DECNet Area, IPX devices are grouped by IPX domain and IP devices are grouped by class A/B/C Subnet.

If you use subnets other than class A/B/C at your site, you may want to create a site-specific subnets grouping. You can create a customized view of IP subnets in your organization in the following way:

- a Add appropriate entries to the SubnetsDB configuration file. See [Appendix D, “Using the SubnetsDB File”](#), for details.
- b Either start a new database or use *Reload Attributes...* with *Subnets* checked to update the attributes of existing devices in the database.
- c Create a new grouping using the following attributes (in the order given):
  - NL Type.
  - Subnet.
  - Deselect *Collapse Redundant Grouping*.
- d Select this grouping.

The IP group will then contain all the devices matching an entry in your SubnetsDB files, grouped by subnet name. The unassigned group will contain the rest of the IP devices, grouped by class A/B/C subnet.

  - **MAC and Type** — This grouping is useful for looking at all the different types of network traffic (for example, IP, IPX, DECNet) being generated by a given physical device.

This grouping is made up of the MAC Address attribute and the NL Type attribute. See [Table 5](#) for more information about these attributes.
  - **Vendor and MAC** — This grouping is useful for identifying devices from different vendors. It is made up of the Vendor attribute and the MAC Address attribute. See [Table 5](#) for more information about these attributes.

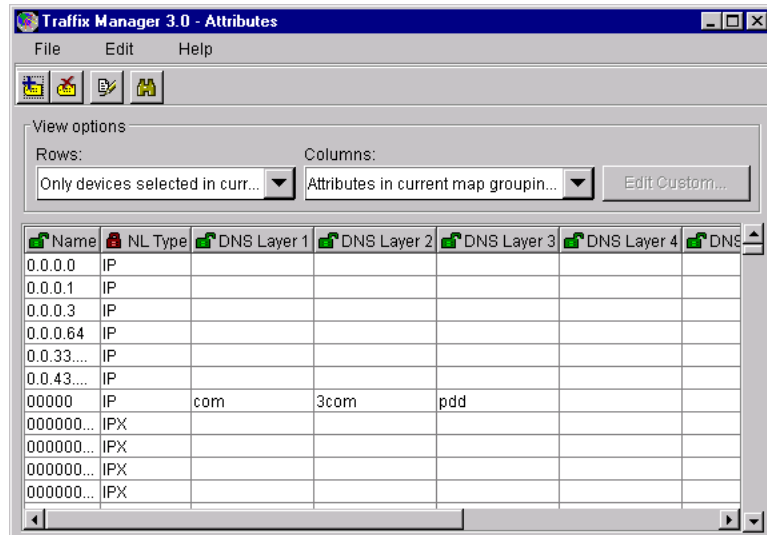
### Creating and Assigning Attributes

You must create attributes, or select predefined attributes, to include in each grouping you want to create.

There are two methods for creating and assigning attributes:

- Set up automatic creation and assignment of attributes using user-defined automatic attribute assignment and your own data sources. See [Appendix E, “Automatic Attribute Assignment”](#) for more information.
- Create attributes and assign values to devices in the Map using the Attributes dialog box. You can create any number of attributes in advance, and then assign values for these attributes to selected devices at any time.

Figure 5 Attributes dialog box



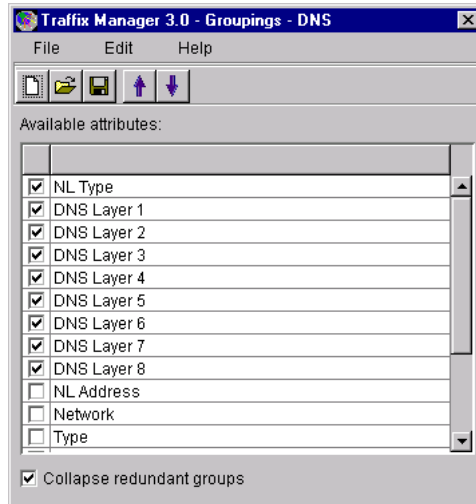
The Attributes dialog box displays, in rows, a list of selected devices on your network, and in columns, a list of available attributes. By default, devices currently selected in the Map are listed, with values for the attributes that apply to the selected grouping. If no devices are selected, the Attributes dialog box displays all devices that are loaded into the Map. You can choose to list the attributes for any grouping.



*You cannot delete an attribute which is included in a grouping. To delete an attribute, you must first remove it from all groupings or delete all groupings which contain the attribute.*

### Creating Groups and Ordering Attributes

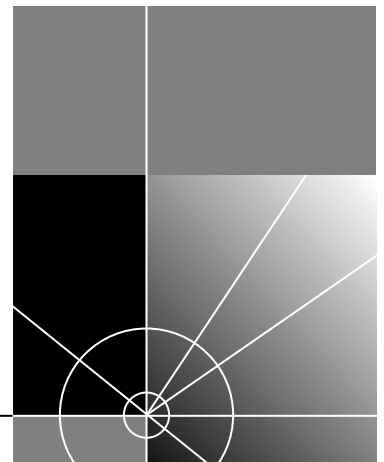
You use the Groupings dialog box to create and manage groupings, and control the order of attributes within groupings. The order in which you place attributes in the Groupings dialog box defines the order in which devices are sorted, and therefore the top-down view of your network.

**Figure 6** Groupings dialog box



# RUNNING TRAFFIX MANAGER

- [Chapter 5](#) [Launching Traffix Manager After the First Time](#)
- [Chapter 6](#) [Configuring Agents for Data Collection](#)
- [Chapter 7](#) [Displaying Network Traffic in the Main Window](#)
- [Chapter 8](#) [Displaying Traffic in Graphs](#)
- [Chapter 9](#) [Using Event Rules](#)
- [Chapter 10](#) [Viewing Events](#)
- [Chapter 11](#) [Overview of Reporting](#)
- [Chapter 12](#) [Report Types](#)







# 5

## LAUNCHING TRAFFIX MANAGER AFTER THE FIRST TIME

This chapter provides information on how to launch Traffix™ Manager, after the first time. It contains the following sections:

- [Launching the Traffix Manager Server](#)
- [Launching a Traffix Manager Client](#)
- [Client Access Levels](#)

---

### Launching the Traffix Manager Server

Start the Traffix server using the Traffix Control Panel. The Traffix Control Panel is also used for database administration. See [Appendix B, “Database Management Using Traffix Control Panel”](#) for more information.

You can launch the Traffix Control Panel by clicking *Start>Programs>Transcend Traffix Manager>Transcend Traffix Manager v3.0 Control Panel*. The Traffix Control Panel can only be run on the server machine. Only one server can be run on a machine at any given time.

For support of multiple servers within the same broadcast domain, see [“Startup Options”](#) on [page 125](#).

---

### Launching a Traffix Manager Client

You can only successfully start a Traffix Manager client if the server is already running. The server may be within the local broadcast domain or outside it. The client is launched from the *Start* menu, and automatically contacts any server that is running in the local broadcast domain.



*If you try to start a Traffix Manager client without launching the server first, you receive an error message.*

To use a remote server, you must add the IP address of the machine running the server to the shortcut in the *Start* menu. To do so, follow these steps:

- 1 Select *Settings* from the *Start* menu, and then *Taskbar...*
- 2 In the Taskbar Properties dialog box, select the *Start Menu Programs* tab.
- 3 Click *Advanced...*
- 4 In the *Exploring - Start Menu* window, select the Traffic Manager Client icon.
- 5 Click the right-mouse button and select *Copy* from the drop-down menu that appears.
- 6 Navigate to the Desktop, click the right mouse button and select *Paste* from the drop-down menu that appears.
- 7 Right-click on the Desktop and select *Shortcut* from the *Properties* menu.
- 8 Add **serveraddress <IP address>** to the command line.

---

## Client Access Levels

You can run multiple clients against a single server. No more than 10 Traffic Manager clients can connect to the same Traffic Manager server.

There are two access levels for running the client:

- The Traffic Administrator level allows the user to configure all aspects of the operation of Traffic Manager, such as data collection and report generation. To avoid security conflicts between multiple clients, there can be only one Traffic Administrator logged in at any one time.
- All other clients are read-only and as such can view all collected data and configurations, but not change collection configurations. When you first start the client, you have Traffic Administrator access, if no other clients are logged in as the Traffic Administrator.

You can change to Traffic Administrator access from the User Authorization dialog box, providing no-one else is logged in as the Traffic Administrator at that time.



*If you are a read-only user and attempt a Traffic Administrator level function, such as configuring a new agent, you are prompted to change to the Traffic Administrator, providing there is no other Traffic Administrator logged in at that time. If there is a Traffic Administrator logged in, access to that function is refused.*

# 6

## CONFIGURING AGENTS FOR DATA COLLECTION

This chapter describes how to use Traffix™ Manager to identify and enable RMON agents on your network for data collection.

It contains the following sections:

- [Supported RMON Agents and Interfaces](#)
- [Finding Agents for Data Collection](#)

See "[RMON Overview](#)" on [page 37](#) for more information about RMON agents.

---

### Supported RMON Agents and Interfaces

Traffix Manager supports all agents which implement all the relevant groups of RMON-1 and RMON-2 standards.

Refer to RFCs 1757, 2021 and 2074 for a list of the RMON groups which are retrieved by Traffix Manager:

- RMON-1 Request for Comment:  
`http://www.it.kth.se/docs/rfc/rfcs/rfc1757.txt`
- RMON-2 Request for Comment:  
`http://www.it.kth.se/docs/rfc/rfcs/rfc2021.txt`
- RMON-2 Protocol Identifiers:  
`http://www.it.kth.se/docs/rfc/rfcs/rfc2074.txt`

See [Appendix F](#) for a list of interface types supported by Traffix Manager.

See `http://www.3com.com/network\_management/probe\_interop` for a list of third-party agents which are supported by Traffix Manager.

## Finding Agents for Data Collection

The agents used may be devices with RMON-1 or RMON-2 embedded within them, such as switches or hubs, or they may be dedicated stand-alone RMON probes.

You can search for compatible agents from the startup wizard and from the Configure Agents dialog box. There are two ways of finding agents on your network:

- You can ask Traffic Manager to search your network automatically for compatible agents.
- If you know the IP address and community string of those agents you wish to collect from, you can specify the agent details yourself.



*If you choose not to find agents automatically, you must add at least one agent manually. Traffic Manager cannot begin to collect data unless there is at least one active agent selected.*

You can choose to leave the startup wizard without finding agents to collect network traffic data, and launch the Traffic Manager client with no data collected. This will display an empty Map on your workstation, from which you can perform limited management and configuration tasks. See [“Launching the Traffic Manager Client”](#) on [page 26](#) for further details. You can then add agents for data collection at a later stage without having to go back through the startup wizard. See [“Adding and Editing Agents”](#) on [page 53](#).

## Configuring RMON-1 and RMON-2 Data Sources

Once you have found agents on your network, you can configure those you want to collect data from. All compatible RMON-2 agents which have been found on your network are displayed in the agent tree in the Configure Agents dialog box.

From the Configure Agents dialog box you can:

- Add more agents to collect data from your network. See [“Adding and Editing Agents”](#) on [page 53](#).
- Enable/disable individual agents and agent interfaces for data collection.
- Suspend/resume all data collection. See [“Suspending and Resuming Data Collection Manually”](#) on [page 54](#).

To enable you to manage large numbers of collection agents, agent folders can be created in the tree and the agents dragged and dropped into them.

## Adding and Editing Agents

From the Configure Agents dialog box you can use Traffix Manager to automatically find agents on your network, or you can add agents yourself. You can then add these new agents to the list in the agent tree. To add an agent manually you need to know the IP address and community string of each new agent.

Community strings, also known as community names, are used to limit access to an agent's *MIB*. The MIB becomes accessible only to a selected set or *community* of management workstations. Management stations require level 4 access to MIBs. Level 4 provides the highest level of access. See [Table 6](#) for more information.

**Table 6** Community Access Levels

Level	Description
1	Read access to MIB-II objects (SNMP MIB)
2	Read access to MIB-II, RMON-1 and RMON-2 MIB and Configuration MIB objects.
3	Read access to MIB-II, RMON-1 and RMON-2 MIB and Configuration MIB objects. Write access to RMON-1 and RMON-2 MIB and Configuration MIB objects.
4	Read and write access to all MIB-II, RMON-1 and RMON-2 MIB and Configuration MIB objects.

A duplicate agent is one with the same IP address and community name as another agent in the agent tree. Traffix Manager does not support duplicate agents. Duplicate error checking is handled by the Add Agent dialog box. If an invalid (duplicate) IP address or community string is entered, an error message appears.

When Traffix Manager retrieves agent details, a list of the interfaces on that agent is displayed. You select the interfaces you wish to collect data from, and add the newly-configured agent to the agent tree.

The agent will be added to the currently selected agent folder in the tree. If no folder is selected, the agent will be added to the top-level *All* folder.

## Viewing Agent Statistics

You can view the statistics of a selected agent from the Agent Statistics dialog box. This dialog box displays various statistics related to SNMP communication with the agent. Refer to the online help for more detailed information about the Agent Statistics dialog box.

## Polling for Data Collection

Traffic Manager collects data periodically once compatible RMON-1 and RMON-2 agents have been located on your network. The standard polling interval is 30 minutes.

Any agents not responding are shown with different icons in the agent tree.

## Polling Agents Over a WAN Link

Using the Advanced Interface Setup dialog box, you can reduce the amount of time Traffic Manager spends collecting data. Refer to the online help for the Advanced Interface Setup dialog box for more information.

## Suspending and Resuming Data Collection Manually

You may want to suspend data collection if you have collected sufficient data to give you a clear picture of the normal level of traffic on your network.

You enable or disable individual agents for collection using the agent tree in the Configure Agents dialog box. You can also suspend and resume collection for all enabled agents from this dialog box. This option is a “master switch” for all enabled agents.

## Downloading Agent Firmware

See [Appendix G](#) for information on why you should always run the most up-to-date version of management software (*firmware*) for the 3Com agents on your network. For instructions on how to download the latest version of firmware, refer to “How do I download new firmware to the agent?” in the online help.

## Setting Operational Mode on 3Com Standalone RMON-2 Agents

The current mode of the agent is displayed in the Agent Maintenance dialog box. 3Com recommends that you use the *RMON-2 Traffic Mode*, because this sets tables on the agent to an appropriate size for use with

Traffic Manager. See [Appendix G](#) for more information about setting the mode on 3Com standalone RMON-2 agents.





# 7

## DISPLAYING NETWORK TRAFFIC IN THE MAIN WINDOW

This chapter contains the following sections:

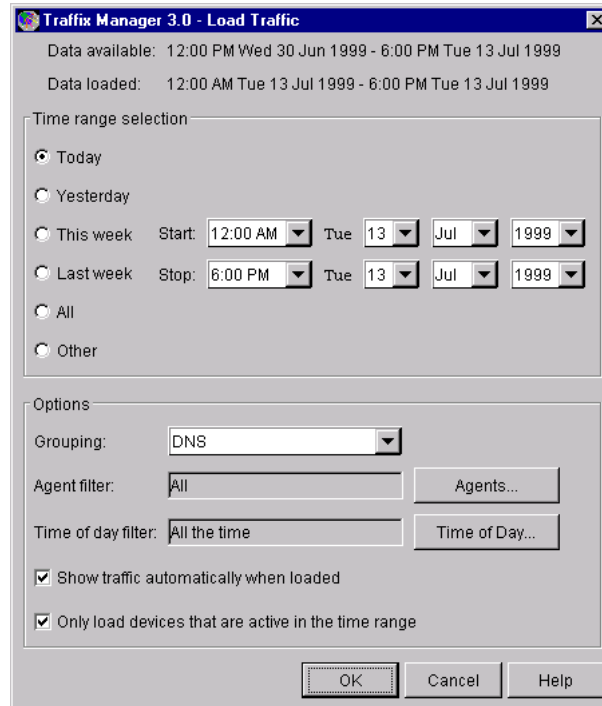
- [Loading Network Traffic Data](#)
- [Working with Objects in the Main Window](#)
- [Displaying Network Traffic Data](#)
- [Protocols, Applications and Favorites](#)
- [Device Aggregation](#)

Before you can display traffic data, you need to use Traffix™ Manager to collect it from your network. To find out if there is data already collected, open the Load Traffic dialog box from the *File* menu. If no data has been collected, see [Chapter 6, “Configuring Agents for Data Collection”](#) for information about collecting data from your network.

---

### Loading Network Traffic Data

You can select how to load and display traffic data in the main window. You make these selections in the Load Traffic dialog box.

**Figure 7** Load Traffic dialog box

## Working with Objects in the Main Window

Once you have loaded network traffic data, you can display information about objects on your network, search for and select objects, and locate objects in the Map.

### Displaying Object Information

There are three types of object information available:

- Device names
- Group and device status
- Group statistics

### Group/Device Status

The color of a device icon and the perimeter color of a group in the Map reflect the status of that object.

- **Grey** — Inactive
- **Green** — Transmitting traffic only
- **Yellow** — Receiving traffic only
- **Orange** — Transmitting and receiving traffic



*A selected object is colored blue. The shade of grey used to color the inside of a group is only used to make it more visible in the Map and does not denote a specific state.*

### Group Statistics

You can use the Number of Devices dialog box to find out how many devices are in a selected group, and how many of those devices are active (transmitting/receiving traffic).

Refer to the online help for the Number of Devices dialog box for more information.

### Searching for Objects

You can search for objects using either the search bar located above the Object List, or the Find dialog box.

Refer to “How do I display network traffic in the Map?” in the online help for more information.

### Selecting and Deselecting Objects

You can select objects directly in the Object List or Map by clicking on them.

### Locating Objects in the Map

For detailed information on locating objects and zooming in on objects and areas in the Map, refer to “How do I display network traffic in the Map?” in the online help.

---






## Displaying Network Traffic Data

Once traffic has been loaded, select the objects for which you want to see traffic. You can display data in one of two ways:

- In the Load Traffic dialog box check *Show traffic automatically when loaded* to show all conversations on the Map automatically when traffic data is loaded.
- Use the *Add Connections To and From* or *Add Connections Between* options from the toolbar to display traffic in the Map as required.

[Table 7](#) describes the traffic display options available from the *Display* menu and from buttons in the main window.

**Table 7** Description of Display Buttons

Button	Function
	<p><b>Add Connections To and From</b></p> <p>Shows all traffic connections going to and from the selected objects to any other objects on the network. Use to determine who the selected objects are talking to.</p>
	<p><b>Remove Connections To and From</b></p> <p>Removes all traffic for the selected objects on the Map.</p>
	<p><b>Add Connections Between</b></p> <p>Shows traffic connections going between the selected objects only. Use to:</p> <ul style="list-style-type: none"> <li>■ Map connections between specific devices</li> <li>■ Map connections within a group</li> </ul>
	<p><b>Remove Connections Between</b></p> <p>Removes traffic connections between selected objects on the Map.</p>
	<p><b>Remove All Connections</b></p> <p>Removes all traffic from the Map regardless of what is selected.</p>

### Displaying Connections Between Objects

With two or more objects selected, click *Add Connections Between* to display traffic going between the selected objects only.

With a single group selected, selecting *Add Connections Between* maps traffic going between objects within that group only.

### Displaying Connections To and From Objects

With an object selected, select *Add Connections To and From* to map network traffic going to or from the object.

If you select a group, the traffic to and from all objects within the group is mapped.

**Combining *To and From* and *Between***

You can use the *To and From* and *Between* options in combination to turn off a subset of the traffic connections.

**Removing and Hiding Traffic**

To remove all traffic from selected objects in the Map, select *Remove All Connections* from the *Display* menu.

To hide all traffic in the Map, select *Hide Mapped Connections* in the *Display* menu.

---

**Protocols, Applications and Favorites**

After grouping devices, you can filter the display of network traffic further, to view traffic carried by selected protocols only.

For example, it may be corporate policy that a specific department should not access the Internet during working hours. You can view web traffic for the department to see if there is any activity at that time.

Traffic Manager provides two ways to define protocol filters so that you can select and view network traffic at higher levels of abstraction. These are *applications* and *favorites*.

An application is a folder containing one or more protocols. Applications are used to make encapsulated protocols easier to select and therefore enable you to monitor a particular type of traffic more easily.

Traffic Manager contains a number of applications, which should be sufficient for most uses, although you can add your own if necessary.

A *favorite* is a folder that can contain both applications and protocols. For example, you could set up a favorite called *Business Critical* that contains applications such as *snmp*, *netes* and *nfs*, in order to view your most critical network traffic.

Traffic Manager contains the following predefined favorites:

- All applications
- All protocols
- Web applications

You can also add your own favorites as required. Favorites can contain other favorites.



*If you want to change the protocols in an application, create a new favorite rather than edit a predefined application grouping.*



*The concept of having applications and favorites (collections of related protocols) also applies also to graphs, reports and events, as well as to viewing in the Map. See [Chapter 8, “Displaying Traffic in Graphs”](#), [Chapter 9, “Using Event Rules”](#), and [Chapter 11, “Overview of Reporting”](#) for further information.*

## Protocol Tools

You can launch the Protocols dialog box by clicking *Protocols* on the *Display* menu. From the Protocols dialog box, you can select applications and favorites to be displayed in the Map, and save selected applications as a favorite.

Using the Configure Protocols dialog box, you can:

- Set up and edit applications and favorites. You can move protocols to an application by selecting and moving them in the Protocols tab of the Configure Protocols dialog box, and moving them into the Applications tab. You can add applications and protocols to a favorite in the same way.



*Two applications cannot contain the same protocol (a protocol can appear in more than one favorite, however). As applications do not overlap, you can display all applications in the Map simultaneously, by selecting the predefined favorite All Applications.*

- Change the color used to denote an item — protocol, application or favorite — in the Map. Setting a color will total up all the lower-level contents of the selected item, and display only the total traffic as one color. Setting the color to *No Color* is a special case, which displays the lower-level contents of the selected item. You can think of this as looking *through* the item to see the contents below.

## User-defined Protocols

It should not be necessary to alter any of the predefined protocols. You can add user-defined protocols if required.

For example, you might want to monitor the use of a particular server that uses two port numbers to communicate with clients on the network. You could add two user-defined protocols to those agents on your network that support user-defined protocols. You can then monitor all interactions between clients and the server using the Map and/or the reporter.

You might then create a favorite called *Server*, containing both user-defined protocols. You could display this favorite in the Map as a single color, to show the overall use of both protocols on your network.

To set up a user-defined protocol, you need:

- The name of the *parent* protocol over which it runs, for example `TCP`.
- The protocol number. For example if the protocol runs on `TCP` port 678, the protocol number is 678.
- The name for the protocol.

From the Configure Protocols dialog box with the *Protocols* tab selected you can also:

- Register a user-defined protocol with an agent so that the agent collects data from the new protocol. If you have created a protocol that is registered with one agent, you can use this option to register it with another agent.
- Deregister a user-defined protocol with an agent so that the agent no longer collects data for the protocol.
- Check whether a specific protocol is registered with an agent.

### Notes on User-defined Protocols



*There are some limitations on the user-defined protocols which 3Com agents support. Refer to the firmware documentation for lists of the 3Com protocols and user-defined protocols that this firmware supports.*

*Data collected using newly defined protocols does not appear immediately in the Map, but only after further data collections have taken place. Data collection is described in [Chapter 3, "Collecting Data"](#).*

*The protocol directory on an agent may be reset when the agent is reset, in which case you must remember to set up user-defined protocols again. The supported 3Com agents listed in the firmware documentation are reset when new firmware is downloaded or the operational mode is changed. See [Appendix G, "Configuring 3Com Standalone RMON-2 Agents"](#) for more information.*

### RMON-2 Limitations

- You can only create protocols as the *children* of existing protocols supported by the agent.

- You can only create child protocols if the protocol you are extending supports the addition of child protocols.



*Many current implementations of RMON-2 agents do not support user-defined protocols. If in doubt, check with your agent vendor.*

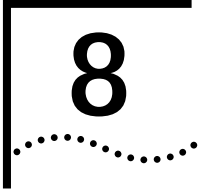
---

## Device Aggregation

Aggregation is a way of limiting the number of devices Traffic Manager has to track. As more devices are displayed in the Map, it becomes more difficult for you to determine traffic patterns on your network. Aggregation reduces the amount of memory and disk resources required by collating data which has been collected.

See [Appendix C, “Aggregating Devices”](#) for a description of default aggregation and information on specifying an aggregation policy.





# DISPLAYING TRAFFIC IN GRAPHS

This chapter contains the following sections:

- [Overview](#)
- [Using the Graph Panel](#)
- [Using the Launch Graph Dialog Box](#)

---

## Overview

You can use the graph tools in Traffix™ Manager to analyze mapped traffic. The graph panel of the main window shows summary information about the most significant items selected in the Map. In addition to this, you can open the Launch Graph dialog box to display more detailed information about selected items.

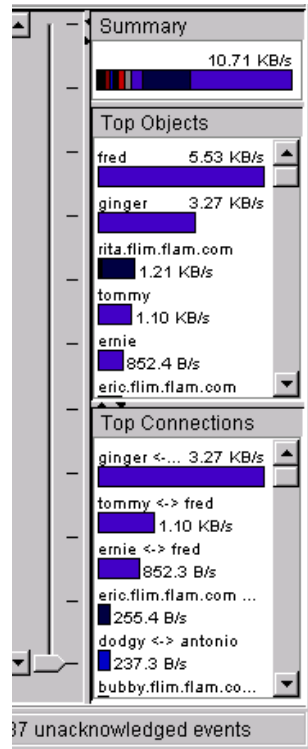
When configuring graphs, consider the following factors:

- **Grouping** — Graphs are used to analyze mapped traffic. They are therefore dependent upon the grouping currently applied in the Map. Grouping is described in [“Groupings”](#) on [page 42](#). The default groupings provide good data for basic analysis.
- **Level** — Panel graphs are generated for the level currently applied in the Map only. The level refers to the hierarchy imposed by the selected grouping, and equates to the attributes in that grouping. For example, the levels within a geographic grouping could be `country` or `city`. For launched graphs, you can select different levels from the Graph Settings dialog box.
- **Connections** — You can only generate graphs showing data for connections displayed in the Map.

## Using the Graph Panel

The Graph Panel of the main window shows basic information about the network activity of selected items in the Map as a number of graphs.

**Figure 8** Graph Panel



The following graphs of objects selected in the Map are displayed in the main window:

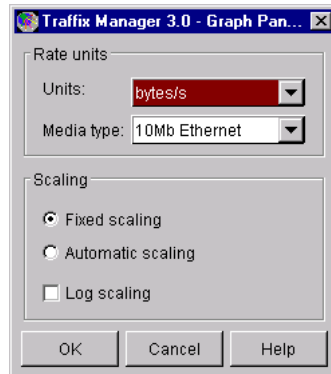
- **Summary Bar** — Shows the sum of all the traffic displayed in the Map for the object(s) selected in the Map.
- **Top Objects** — If a single group is selected in the Map, this graph shows the busiest objects in the selected group at the level selected in the Map.

If more than one object is selected in the Map, this graph shows the busiest of the objects selected.

- **Top Connections** — Shows the busiest connections involving the objects selected in the Map.

Use the Graph Panel Settings dialog box to configure the display of the Graph Panel.

**Figure 9** Graph Panel Settings dialog box



The options for display are:

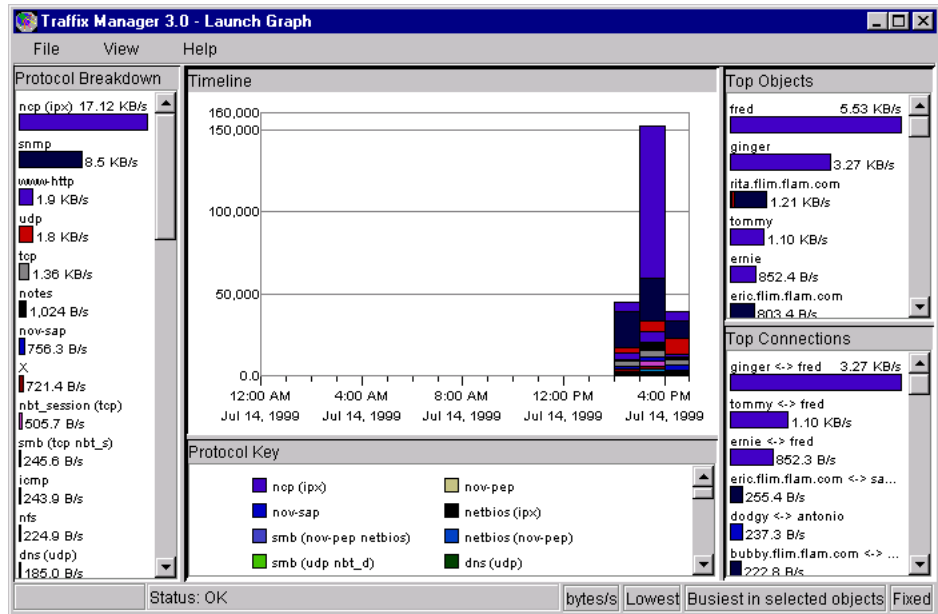
- **Units** — The unit of measurement used when calculating the charts:
- **Media Types** — Only active if *bits per second* or *% utilization* are selected in the Units field.
- **Fixed/Automatic/Logarithmic scaling** — If automatic scaling is selected, Traffic Manager adjusts the size of the bars in each chart to fill the space available.

---

## Using the Launch Graph Dialog Box

Use the Launch Graph dialog box to display detailed information about items in the Map.

Figure 10 Launch Graph dialog box



The settings used to create the launched graph are those used in the Map at the time you launch the dialog box. If the data is filtered in some way, for example by protocol, that filtering is used when producing the graphs.



*Each graph will only use the connections which are plotted and displayed in the Map when the graph is launched.*

You can display multiple instances of the dialog box — to compare data for various protocols or connections, for example.

The Launch Graph dialog box has five main areas:

- **Protocol Breakdown** — Each of the bars shows the total for each protocol of the filtered traffic for each of the selected objects.
- **Timeline** — Shows the traffic generated over the time period loaded into the Map.
- **Protocol Key** — This indicates which color denotes each protocol. (You can set the colors using the Configure Protocols dialog box described in [“Protocol Tools”](#) on [page 62.](#))

- **Top Objects** — Show the busiest objects. Which objects are considered depends on the level set in the Graph Settings dialog box.
- **Top Connections** — Shows the busiest connections. Which connections are considered depends on the Level and Unit Total set in the Graph Settings dialog box.

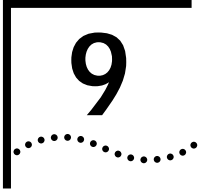
Because the necessary calculations can be lengthy, the status bar at the bottom of the Launch Graph dialog box shows a progress bar. When the progress bar is full, Traffic Manager has finished calculating the charts.

## Graph Settings

You use the Graph Settings dialog box to control the display of charts in the Launch Graph dialog box. The options are:

- **Scope** — The comparative point of reference for all the connections. If devices or groups are selected in the Map, you can produce a graph for either the *Busiest Talkers* among the objects selected, the *Busiest Listeners* or the *Busiest Link*. If a connection is selected in the Map, you can produce a graph for the traffic going in either or both directions between the two objects.
- **Units** — The unit of measurement used when calculating the charts.
- **Media Type** — Only active if *bits per second* or *% utilization* are selected in the Units field.
- **Fixed/Automatic/Logarithmic scaling** — If automatic scaling is selected, Traffic Manager adjusts the size of the bars in each chart to fill the space available.





# USING EVENT RULES

This chapter describes how to use event rules to analyze the data collected by Traffix™ Manager and to inform you of traffic changes on your network.

This chapter contains the following sections:

- [Overview](#)
- [Predefined Event Rules](#)
- [Examples of Event Rules](#)
- [Configuring Event Rules](#)
- [Using Event Rules](#)

---

## Overview

Using Traffix Manager, you can set up event rules to provide you with information about the security of your network, and the level of traffic on the network. Event rules are applied to traffic data as it is collected. When the conditions of a rule are met, Traffix Manager generates one or more events which you can view in the Event List.

See [Chapter 10](#) for more information on viewing events and analyzing the causes of events.

Rule-based event generation provides you with the following benefits for proactive network monitoring:

- It enables you to monitor security policies without having to examine map data manually.
- It provides you with a configurable way of automatically analyzing collected data, informing you when unusual events occur.
- It gives you an easy way of producing related map and graph displays when events occur, without complex configuration.

The event rules in Traffix Manager fall into two broad categories:

- **Security** — An event is generated when some aspect of network security may have been compromised.
- **Traffic** — An event is generated when a significant change in traffic patterns is detected.

The various types of event rule are discussed in more detail in the following section.

Traffix Manager provides a number of predefined event rules that cover common network issues. You can also add your own event rules, edit existing event rules and enable/disable them, as described in [“Configuring Event Rules”](#) on [page 75](#).

The final part of this chapter suggests ways of using the various types of event rule to implement strategies for managing your network.

---

## Predefined Event Rules

Traffix Manager is supplied with a number of predefined event rules, which are applicable to most networks. These event rules generate events when significant changes occur on the network. They are:

- Detect new devices on the local network
- Detect changes on the local network
- Check for abuse of the Internet connection
- Detect WEB traffic during working hours
- Monitor local Notes server traffic
- Monitor local DNS server traffic
- Monitor local NFS server traffic
- Monitor local web server traffic
- Monitor local SMB (Microsoft) server traffic
- Monitor local NCP (Novell) server traffic



*Local devices are defined in terms of the local DNS domains in which they reside. See [“Local Domain Specification”](#) on [page 130](#) for more information.*



---

## Examples of Event Rules

There are a total of eight types of event rule, the possible uses of which are discussed below.

### Security Event Rules

These types of event rule help you to protect your network from unauthorized access or improper use.

#### **Detect Unauthorized Machine Access**

You use this type of event rule to help you enforce policies about access to specified machines. A device or devices are 'protected' by an event rule of this type, so that an event is generated whenever an unauthorized machine accesses one of these devices. The event rule can be restricted to monitor traffic for specific protocols only.

For example, you can use this event rule to detect anyone accessing the e-mail server from outside the local network.

#### **Detect Network Misuse**

You use this type of event rule to prohibit or limit certain access to the network at certain times. An event is generated if traffic is detected during the prohibited time. You can limit the event rule to monitor specific parts of your network or specific protocols.

For example, you can use this event rule to:

- Detect any traffic other than backup traffic on the WAN link at night.
- Detect anyone using the Internet at the weekend.

#### **Detect Network Sweep Attack**

This type of event rule generates an event if an outside user attempts to discover devices on your local network by scanning a range of IP addresses. This could indicate that the user is planning to gain access to your network.

#### **Detect New Devices**

An event is generated if a new device is discovered. This type of event rule is activated only after collection has been running for several hours, preventing spurious events from cluttering the Event List. The event rule can be restricted to monitor specific groups.

## Traffic Event Rules

These types of event rule help you to detect significant changes in the behavior of a machine or connection. Such changes are often causes or indicators of problems on the network. They may also indicate that some part of the network is overloaded, and could give advance warning that the load on a device is increasing.

### Monitor Network Resource Usage

You use this type of event rule to detect machines that are using more than their share of the network. You can configure an event rule to monitor the whole network, individual devices or specific WAN links.

When an event rule of this type is active, Traffix Manager estimates the available bandwidth of the network, device or WAN link that is being monitored. If one machine uses up more than a certain percentage of the available bandwidth, then an event is generated.

By applying the protocol filter to an event rule of this type, you can use it to monitor the usage of specific network services.

For example, you can use this event rule to:

- Monitor for devices which use an excessive amount of Novell bandwidth.
- Monitor for devices which are using the Internet connection excessively.

### Monitor Critical Devices

You use this type of event rule to monitor a set of devices and generate an event if the network traffic of those devices changes significantly. You can spot changing loads on server machines, and prevent problems with response times and overloading.

Once data collection has begun, you can start to build up a picture of typical traffic patterns and network usage. Based on this information, Traffix Manager will automatically guess which are the critical devices on your network. However, you will get more predictable results from this event rule if you specify server devices yourself.

An event rule of this type can detect changes in the traffic levels of a device, and changes in the usage of different protocols. It works by comparing the present activity of the specified devices with their historical behavior.

By applying the protocol filter to an event rule of this type, you can use it to monitor the usage of specific network services on the devices.

For example, you can use this event rule to:

- Monitor the activity of your e-mail servers.
- Monitor the activity of your router.

### **Monitor Critical Connections**

Changes on an important link can lead to unexpected congestion. You can use an event rule of this type to monitor a list of WAN or backbone links and generate an event if the network traffic on the link changes significantly.

An event rule of this type can detect changes in traffic levels and changes in the usage of different protocols. By applying the protocol filter to this type of event rule, you can use it to monitor the usage of specific network services on the connections.

For example, you can use this event rule to:

- Monitor the activity of your WAN link to another city.
- Monitor FTP traffic activity on the Internet connection.

### **Monitor Network Trends**

You can use an event rule of this type to monitor changing long-term traffic levels on the whole network or on part of the network. Events are generated if significant changes over time are detected. An increase in the overall activity of the network may be an early warning of problems or increased congestion.

By applying the protocol filter to a rule of this type, you can use it to monitor the changing usage of specific network services.

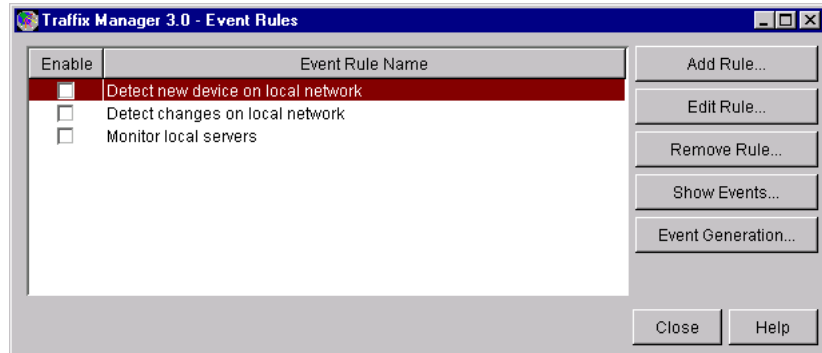
For example, you can use this event rule to:

- Monitor the activity of a specified local network segment.
- Monitor Web traffic activity on the whole network.

---

## **Configuring Event Rules**

You can add your own event rules and edit, enable or disable existing rules according to your own requirements. You use the Event Rules dialog box to do this.

**Figure 11** Event Rules dialog box

Traffic Manager provides wizards to help you add and edit event rules.

## Refining Event Rules

When you add or edit an event rule, you can modify it to monitor the traffic on your network and your network security, according to your own requirements.

### Specifying Devices

You can specify the groups and devices to which an event rule applies. If a group is specified, the rule applies to all devices in that group, unless you specifically exclude a device from the group. The list of devices which you are monitoring through all these rules is therefore dynamic and may change if the devices in the group change.

By default, the grouping used for a rule is that currently applied in the Map. However, once created, a rule always uses the same grouping.

### Selecting Protocols

Typically an event rule applies to all traffic, regardless of the kind of protocol being used. You can restrict the scope of a rule by choosing a specific application or favorite (set of protocols) for a rule to monitor. Traffic of other protocol types is then ignored. See [Chapter 4, “Grouping Network Devices in the Map”](#) for more information about setting up applications and favorites.

You can select a predefined protocol, or make your own protocol selection. See [“User-defined Protocols”](#) on [page 62](#) for more information.

## Specifying the Time Filter

With certain types of event rule, you can specify the times at which rules apply. For example, you could choose to restrict unauthorized traffic at all times, or only during certain periods.

## Specifying Sensitivity

For most event rule types, you can specify how sensitive you want the rule to be:

- **Security event rules** — high sensitivity generally means that only a small amount of prohibited traffic is required for an event to be generated.
- **Traffic event rules** — high sensitivity generally means that events are generated in response to small changes in the behavior of the device, connection or network being monitored.

When you create an event rule, you can set the sensitivity of that rule approximately on a simple slider. However, you might find it easier to create a rule and then adjust its sensitivity in response to the number of events that it generates. The Event List makes it easy for you to adjust the sensitivity of event rules in this way. See [Chapter 10, “Viewing Events”](#), for further information.

To specify sensitivity with more precision, or to understand exactly what the sensitivity of a rule means, open the Thresholds tab in the Sensitivity dialog box in the Event Rule Creation Wizards.

---

## Using Event Rules

Below are some suggestions about configuring event rules to give you more information about the behavior of your own particular network.



*Some of these ideas may not be applicable to your network.*

### Monitoring Your Network as a Whole

#### Spotting General Long Term Trends

You can configure a Monitor Network Trends event rule to generate an event if the usage of your network fluctuates. An event rule of this type, *Detect changes on local network*, is preconfigured.

You could also use a Segment Activity report if you would rather view data on your network periodically. See [“Segment Activity Report” on page 103](#) for more information.

## Maintaining Network Security

You can configure Detect Network Sweep Attack and Detect New Devices event rules to generate security events. There are event rules of both types already preconfigured. However, your *firewall* may be a more appropriate source of information about attacks from outside the network than Traffic Manager.

## Enforcing Corporate Policy About Network Usage

If you want to have specific policies about what the network is used for at different times of day, you might want to consider some of the suggestions under [“Implementing Business Policies”](#) on [page 80](#).

## Monitoring Protocol Usage

You can configure a Monitor Network Trends event rule to monitor the growth of a specific protocol or set of protocols. For example, you might want to be informed if the level of Web traffic increases significantly or goes beyond a specified threshold.

## Monitoring Servers

### Monitoring Changes in Server Activity

If you expect the activity of your servers to be fairly constant, you can configure a Monitor Critical Devices event rule to tell you if the activity of your servers changes unexpectedly. An event rule of this type, *Monitor critical devices*, is preconfigured. See [“Monitor Critical Devices”](#) on [page 74](#).

### Preventing Server Congestion

You can configure a Monitor Network Resource Usage event rule to detect if one machine seems to use an excessive amount of bandwidth on a server. A device activity report or a graph on the map can also be used to provide an immediate summary of which devices are using a server the most. See [“Device Activity Report”](#) on [page 101](#) and [Chapter 8, “Displaying Traffic in Graphs”](#).

### Monitoring Which Devices Are Using A Server

You can track which devices are using a particular server by configuring a Detect Unauthorized Machine Access event rule for that server. When a new device starts using the server, you will be notified through an event rule. If you wish, you can then add the device to the list of users allowed to access that particular server.

The Map can provide you with immediate information about which devices have been using particular servers.

### **Detecting Unauthorized Servers**

You can use the Detect Network Sweep Attack rule to spot users creating unauthorized servers on the network. For example, you can detect unauthorized FTP servers by creating a rule which detects FTP traffic on the network, but which ignores traffic to and from known FTP servers.

## **Monitoring WAN Links and Backbone Links**

### **Monitoring Congestion on WAN Links**

You can configure a Monitor Critical Connections event rule to inform you when a link is becoming congested. You can either set an absolute threshold at a level of traffic which you think is acceptable on the link, or you can use the event rule to tell you when traffic levels on the link change significantly. A Connection Activity report can be used to give you regular information on the activity of a link. See [“Connection Activity Report”](#) on [page 100](#) for more information.

### **Monitoring Single Devices Which are Overusing the Capacity of a Link**

You can configure a Monitor Network Resource Usage event rule to tell you when one device is using a lot of bandwidth on a link. Similar information can be obtained on a regular basis using a Top N Connections report. See [“Top N Connections Report”](#) on [page 105](#) for more information.

### **Detecting Network Misuse**

Sometimes congestion on a link can be caused by misuse. You can configure a Detect Network Misuse event rule to spot users using a WAN link for Web traffic during working hours.

For example, if you know that a connection should only be used for Lotus Notes traffic then you could configure a Detect Network Misuse rule to spot any *application* except Notes. See [Chapter 4, “Grouping Network Devices in the Map”](#) for more information about applications.

If you have a network with multiple servers in different sites, you can configure a Detect Unauthorized Machine Access rule to make sure people access their local server rather than accessing a server across a WAN link.

**Implementing  
Business Policies**

Some organizations and network administrators have specific policies about how the network can be used, in general or at different times of day. Detect Network Misuse and Detect Unauthorized Machine Access event rules are powerful tools for detecting behavior that does not conform to such policies.

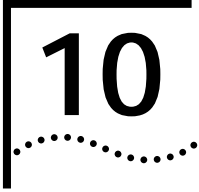
You might require that most of your network bandwidth is available for backups at night. You could configure a Detect Network Misuse event rule to spot significant traffic during the night which is not backup traffic.

You might also require that bandwidth be available on certain links for certain activities at certain times of day. For example, you could use a Detect Network Misuse event rule to spot Web traffic on a WAN link during working hours.

You can create Detect Unauthorized Machine Access event rules to check that only authorized devices access important machines at critical times, for example, during backup.

As all rules have a time filter, you can configure event rules that only apply at certain times of day. For example, you could configure a Monitor Critical Devices event rule to generate an event if the behavior of your backup server changes significantly during the night.





# VIEWING EVENTS

This chapter describes use of the Event List. It contains the following sections:

- [Overview](#)
- [Viewing Events](#)
- [Viewing and Managing Selected Events](#)
- [Forwarding Events as SNMP Traps](#)

---

## Overview

Traffix™ Manager enables you to create event rules about the traffic on your network and network security. When the conditions for a rule are met, an event is generated. See [Chapter 9](#) for information on configuring event rules.

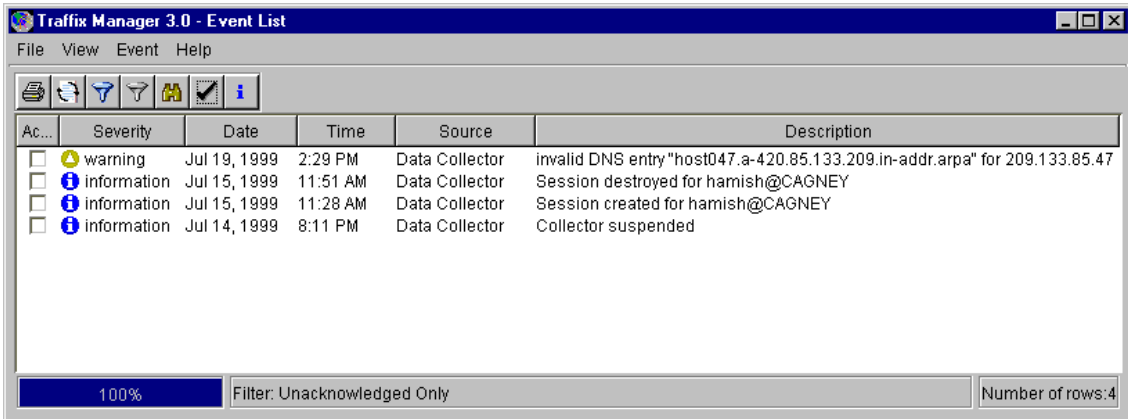
Events are also generated by the Collector and Reporter processes.

The Event List in Traffix Manager displays events generated by all these sources, and supports various viewing options. With the Event List, you can view selected events in greater detail, and use data from an event to drive the display in the Map.

## Viewing Events

You use the Event List to display information about events.

**Figure 12** Event List



The Event List provides the following information about each event:

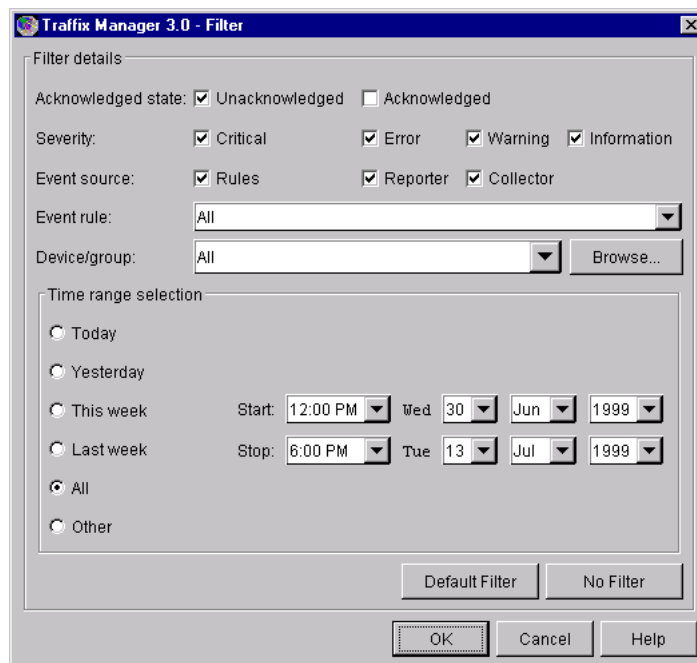
- **Acknowledged** — whether the event has been acknowledged. By default only unacknowledged events are displayed.
- **Severity** — Events are categorized by four levels of severity, information being the least severe, and critical the most severe:
  - Information
  - Warning
  - Error
  - Critical
- **Date** and **Time** the event was generated.
- **Source** — whether the event was generated from the Collector, the Reporter or from an Event Rule. You can choose to display events from one or more sources.
- **Description** of the event.
- **More detail** on the event. Click *More Detail* on the *View* menu to launch the More Detail About Event dialog box. This displays the following:
  - The time the event was logged.

- The severity of the event.
- The rule that generated the event.
- A detailed explanation of the reason for the event.
- The activity of the device before and after the change that caused the event.

You can sort, filter, and summarize the display of events. These last two operations are described in more detail below.

**Filtering Events** You filter event data from the Filter dialog box.

**Figure 13** Filter dialog box



You can filter the event data in a number of ways, including:

- To show only **unacknowledged** events.
- By **severity**.
- By **the source of the event** — Event Rules / Reporter / Collector.

- By **event rule**.
- By **device / group** — You can select a grouping and a group or device. When launched for a particular group or device from the Map, the Event List shows all events in the event log which relate to the selected device or group.



*Only events generated by event rules can be displayed in this way.*

- By the **time period** in which events were generated — today, previous day, previous week, or previous month.
- To a **specific time** — You can specify start and end times for the current view.

## Summarizing Events

You can manage the display of the Event List by summarizing events, so that only one entry is shown for a number of events. When events are summarized, the number of events related to the summarized entry is displayed.



*Events which have been filtered out are not displayed in the summary.*

You can summarize events in one of the following ways:

- **Summarize by device** — You can show the number of events associated with each device that is not filtered out.
- **Summarize by severity** — Shows one entry per severity.
- **Summarize by rule** — Shows one entry per rule.
- **Summarize by day** — Shows one entry per day.
- **Do not summarize.**

## Output of Events

You can output events in the following ways:

- **Export to CSV File** — Saves the contents of the event log to a comma separated value (CSV) format file, which can be read into a spreadsheet or database application. The file name is overwritten each time the event is output.
- **Print.**

---

## Viewing and Managing Selected Events

By selecting an event in the Event List, you can carry out the following actions. These actions do not apply to events generated by the Collector or the Reporter.

- Show detailed information about the event.
- Acknowledge the event.
- Modify the event rule on which the event is based, and increase or decrease the rule's sensitivity.
- Disable the event rule.
- Modify the event rule to ignore the device(s) that caused the event.
- Display the traffic in the Map that caused the event.
- Display a graph of the traffic that caused the event.

The last three operations depend on the type of event, and are described in more detail in the remainder of this section.

### Deleting Events

You cannot manually delete events. Events are deleted automatically after a certain period of time. This is the same amount of time for which trend data is stored. You can specify the maximum amount of disk space that will be used to store this data from the Traffic Control Panel. See [“Database Maintenance”](#) on [page 123](#).

### Ignoring Devices or Connections

You can modify the event rule that generated an event to ignore certain devices or connections. This only applies to events triggered by event rules, and prevents the event being generated in future.

### Displaying an Event in the Map

You can use events to drive the Map. It can display a view representing the traffic that triggered a selected event, depending on the type of the event. This only applies to events triggered by event rules.

### Displaying an Event in the Launch Graph Dialog Box

You can use events to drive the Launch Graph dialog box. The Launch Graph dialog box can display graphs of the data related to the traffic that generated the event (showing two comparative data sets where appropriate). This only applies to events triggered by event rules.

## Forwarding Events as SNMP Traps

By selecting an event in the Event Generation dialog box, you can choose to forward the event as an SNMP trap to your own Open Management Platform (for example, HP OpenView or SunNet Manager).

The Event Generation dialog box allows you to configure the following:

- The severity of events generated by event rules. This allows you to assign different severities to various rules, so that event rules which you consider to be unimportant generate events of “Information” level severity (the least severe), while event rules which you consider to be important generate events of higher severity.
- You can choose to enable/disable events generated by rules and system-generated events of different severities. Therefore, if you are not interested in the informational events from the Collector, for example, you can disable them.

### Configuring Traffic Manager to Forward Events as SNMP Traps

Select an event in the the Event Generation dialog box to forward as an SNMP trap to your own Open Management Platform (OMP). You can enter the trap destination as an IP address or DNS name. The generated event appears in the event viewer for the OMP.

### Integrating Traffic Manager SNMP Traps with HP OpenView

This section gives an example of how to integrate Traffic Manager SNMP Traps forwarded from the Event List with HP OpenView. At the time of writing, the Traffic Manager Event forwarding feature uses the 3Com RMON Event Trigger SNMP Trap PDU (Specific ID 82).

### Configuring an Open Management Platform (OMP)

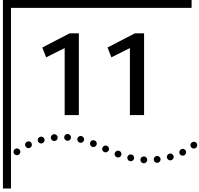
This example refers to HP OpenView Network Node Manager 6.0 for Windows NT. Alarms are generated when Network Node Manager receives events.

- 1 To create a new Alarm Category for Traffic Manager events, follow these steps:
  - a Click *Event Configuration* in the *Options* menu to open the Event Configuration dialog box.
  - b Click *Alarm Categories* from the *Edit* menu.
  - c Enter *Traffic Manager* in the Name field.
  - d Click *Add*.

- 2 The MIB files that define events are supplied by a number of enterprises. Select *3Com* in the Enterprises field of the Event Configuration dialog box. The system object ID corresponds to the value supplied with the SNMP Trap.
- 3 The list in the bottom half of the Event Configuration dialog box lists events associated with the enterprise selected in the top half.  
In the Events for Enterprise 3Com field, double-click *3Com\_RmonEventTrig* to open the Modify Events dialog box.
- 4 To change event configurations, click the Event Message tab and complete the following fields:
  - a Select *Log and display in category* in the Actions field.
  - b Select *Traffic Manager* in the Log and display in category list.
  - c Select a severity level to control the severity rating that Network Node Manager assigns to this alarm.
  - d Do *not* edit the Event Log Message field.
- 5 You can define actions for Network Node Manager to perform automatically whenever a specific event is received. Click the Actions tab and complete the following fields:
  - a In the Command for Automatic Action field, enter the following:  
**cmd /c mplay32 /play /close  
%SystemRoot%\Media\Office97\ Driveby.wav**
  - b In the Popup Window Message field, enter the following:  
**Sweep Attack has occurred!!! Check Traffic Manager  
to snag offender**







# OVERVIEW OF REPORTING

This chapter contains the following sections:

- [Overview](#)
- [Managing Reports](#)
- [Strategy for Reporting](#)
- [Effects of Grouping on Reports](#)

---

## Overview

You use the reporting tools in Traffix™ Manager to produce professional, multi-page reports from collected data about the traffic in your network. There are eight types of report, incorporating over 40 different charts that can extract and display the most significant information about traffic during a specified period.

You can schedule the generation of daily, weekly and monthly reports. These reports are automatically run overnight and delivered to your Web server or printer, or stored as data files for later use.

You can also generate reports on demand (*ad hoc* reports) at any time.

## Types of Report

Reporting focuses on four kinds of object: connections, devices, groups of devices, and segments. For each kind of object there are two types of report, activity and top N, making the total of eight different types of report.

Each report type therefore specifies which objects are reported on and what level of detail is given in each report.

- Use activity reports to give detailed information about one or more specified objects.

- Use top N reports to determine and report on the most active objects on your network. Here, N is a number between 1 and 50 that you can choose for each report.

The different types of report are detailed in [Chapter 12](#).

### Report Instances

You can set up reports for your specific needs. To set up a report, you add an *instance* of a selected report type, specifying which objects to report on. For example, you might set up a top N report on the top 10 devices in Europe. You can then schedule the report to be run daily, weekly or monthly. Alternatively, you could generate an *ad hoc* report when you require one.

When a report is run, either by Traffic Manager at a scheduled time, or *ad hoc*, raw data is generated. You can output or view raw report data as many times as you require, without having to regenerate the report.

### Output

Traffic Manager uses the raw data to output professional reports as hard copy to a printer on the server, as HTML files, or as Comma Separated Value (CSV) files. CSV files can be read into a spreadsheet or database application for further analysis.

See [“Setting Output Options”](#) on [page 95](#) for more detail.

### Periods Covered by Reports

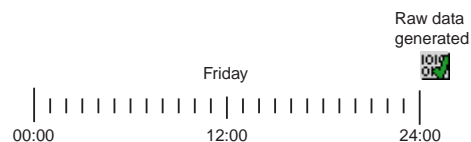
There are three standard report periods: daily, weekly and monthly.

#### Daily Reports

These reports use all data collected on the specified day (from 00:00 to 24:00) and are generated in the early hours of the following morning.

For example, if you select Friday ([Figure 14](#)), the report is generated early on Saturday morning.

**Figure 14** Time Line for Daily Report Generation

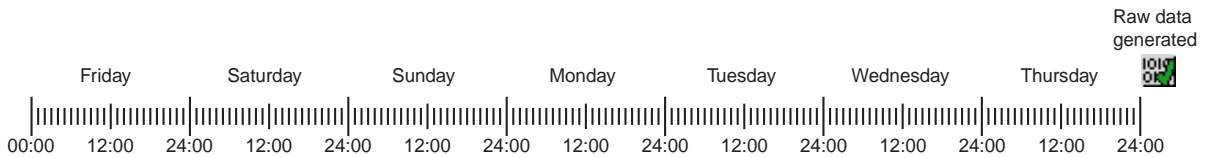


### Weekly Reports

These reports use all data collected on the day specified and the following 6 days. The report is generated in the early hours of the day after the last day covered by the report.

For example, if you select from Friday through to the following Thursday (Figure 15), data covering the 7 days from 00:00 Friday to 24:00 Thursday of the following week is used. The report is generated in the early hours of Friday morning. Therefore the selected day is the first day covered by the next weekly report *and* it is the day on which the previous week's report is ready for viewing.

**Figure 15** Time Line for Weekly Report Generation

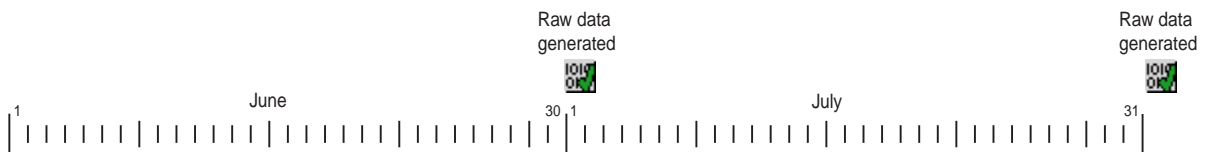


### Monthly Reports

These reports use data collected on the specified day of the month and the calendar month following (including that day). The report is generated in the early hours of the day following the last day covered by the report.

For example, if you select from the first day through to the end of each month (Figure 16), the raw data for the whole of June (June 1st 00:00 to June 30th 24:00) is covered by the report. The report is run in the early hours of July 1st. Again, the selected day of the month is the first day covered by the next monthly report *and* it is the day on which the previous month's report is ready for viewing.

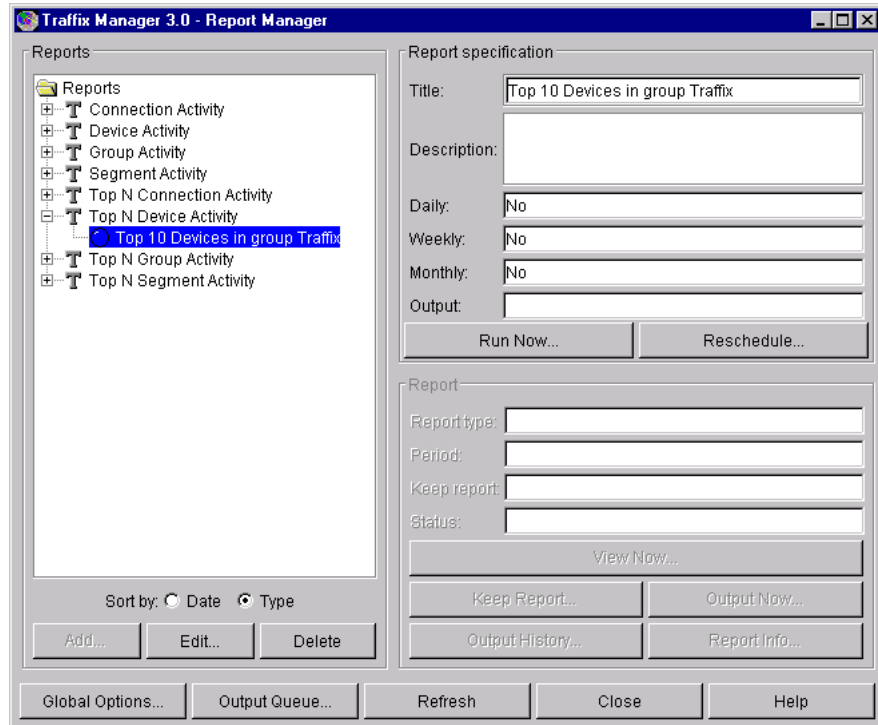
**Figure 16** Time Line for Monthly Report Generation



## Managing Reports

You use the Report Manager to add, schedule, edit and delete reports.

**Figure 17** Report Manager



The Report Manager has three main areas:

- **Reports** — Displays a tree of report types, instances, raw data, and output. You can add, edit and delete items in the tree. You can display reports by the Date they were created, or by Report Type.
- **Report Specification** — Displays a summary of key information about a report instance. You can reschedule reports and run *ad hoc* reports.
- **Report** — Displays a summary of key information about raw report data or HTML output. You can output and view reports and display detailed output status information.

The use of these three areas in managing reports is explained in more detail in the remainder of this section.



The reporting features available depend on the client access level. A read-only user can browse existing reports, view report details, and view reports in the output queue. An administrator can also add, edit and delete reports, change report scheduling and output options, and run ad hoc reports. See [“Client Access Levels”](#) on [page 50](#) for further information about access levels.

## Creating, Editing and Deleting Reports

You use the reports tree in the Reports area to carry out these tasks. There are four levels within the tree:

- **Report types** — The eight report types are listed (see [Chapter 12, “Report Types”](#) for a detailed description of each type of report).
- **Report instances** — Each report instance appears as a child of its original report type. You can add a new report instance based on a selected report type, and edit, reschedule and delete report instances.

You can display a summary of key information about the configured report instance and scheduled generation and output. See [“Interpreting Summary Information”](#) on [page 94](#) for more information.

When you add a report instance, the grouping currently applied in the Map is used.

- **Raw data** — Each time a report instance is run, either scheduled or *ad hoc*, Traffic Manager stores the raw report data in the relational database. The raw data is shown as a child of the report instance, and labeled with the date it was run.

You can select the raw data for any date of interest and re-output it or view it as required.

Raw data is gathered for a specific time period according to the schedule set up for a report instance. At each scheduled generation point, a new raw data entry is added. For example, if you add a top N devices report instance to be generated daily, seven raw data entries are added in one week.

Each raw data icon is marked with a tick if generated successfully, or with a cross if its generation failed. (Generation could fail if, for example, the database is full. See [“Troubleshooting Reports”](#) on [page 116](#) if necessary.)

You can also display a summary of key information about the raw data. See [“Interpreting Summary Information”](#) on [page 94](#) for more information.



You can choose to delete raw data to reclaim disk space if required. See [“Setting Global Report Options”](#) on [page 96](#) for more information about deleting raw report data.

- **Report output** — If you have scheduled the output of a report instance as HTML, the generated HTML output is shown as a child of the raw data.

You can display a summary of key information about the HTML output. See [“Interpreting Summary Information”](#) on [page 94](#) for more information.

You can choose to keep raw report data and HTML output files indefinitely, or automatically delete them after a specified period. See [“Setting Global Report Options”](#) on [page 96](#) for more information.

### Scheduling Reports

The Report Schedule dialog box is displayed automatically when you add a new report instance. Use this dialog box to schedule the report period: daily, weekly or monthly. You can reschedule reports at any time.

If you do not specify a report period, the report instance is saved in the Report Manager, but no raw report data is gathered and no reports are output. You can use a report instance that is saved without scheduling output to generate *ad hoc* reports, or you can later reschedule it.

### Rescheduling Reports and Running *Ad Hoc* Reports

You use the **Report Specification area** of the Report Manager when carrying out these tasks. Use the *Run Now* function to generate an *ad hoc* report.



*Reports may take some time to generate and so may not be available immediately. Other reports may be running or there may be a queue of reports waiting to be run.*

### Managing Raw Data and Report Output

A summary of the key information for the selected raw data or HTML output entry is displayed in the **Reports area** of the Report Manager. You can also view the selected output in a Web browser, change the data lifetime and display status information about the report instance and outputs.

#### Interpreting Summary Information

- **Report Type** — Whether the selected entry is raw report data or HTML output.

- **Period** — The time range covered by the selected raw data or output.
- **Keep Report** — The date the report is to be deleted, or *Keep Forever*, if the report is to be kept indefinitely.
- **Status** — Whether raw data or output was generated successfully. To display the generation history for reports, see [“Monitoring Report Generation and Output”](#) on [page 96](#).

### Setting Output Options

You can specify one of three output options in the Report Schedule dialog box:

- **HTML** — When the report is run, an HTML file which can be displayed using a Web browser is generated. Use the Traffic Control Panel to configure the directory for HTML output files. See [Appendix B, “Database Management Using Traffic Control Panel”](#), for further information.



*If you wish to serve the directory used to store HTML files to your Web server, make sure the directory is visible to your server and has the necessary permissions.*

*If you wish to link to the overall index page generated for HTML reports, the file name is `index.html` in the chosen reports output directory.*

- **Printer** — When the report is run, a graphical report including contents page is printed.

Reports can be delivered automatically only to a printer visible to the server. If you want to print a report using a printer visible to the client, you should output the report as HTML. You can then print the required pages from your Web browser.

- **CSV file** — Saves the report contents to a CSV format file on the server, which can be read into a spreadsheet or database application. The specified file is overwritten without warning each time the report is output.

### Viewing HTML Output

Traffic Manager launches your default Web browser to view HTML output for a report. If you choose to view raw data for which no HTML output file exists, the output file is first generated by Traffic Manager.



*HTML output generation may take some time, according to the amount of data being processed.*

### Monitoring Report Generation and Output

Use the Output Queue to view output requests that are due to be run, that are complete, or have failed. (Report output could fail if, for example, a file cannot be written to, or a printer is off line. See [“Troubleshooting Reports”](#) on [page 116](#) if necessary.)

You can show output for all reports, or only for the report currently selected in the Report Manager. There are separate queues for the generation of raw data and the output of reports.

Raw reports can take a considerable time to generate, and so a backlog of reports waiting to be run may build up. If necessary, you can select output requests that have not yet been run and delete them — in order to run an *ad hoc* report immediately, for example.

### Setting the Lifetime of Raw Report Data

On a per-report basis, you can specify whether to keep that particular raw report data indefinitely, or you can use the Global Options dialog box to change the lifetime of that raw report data or output.



*If your global policy is specified in the Global Options dialog box as Keep Forever, you cannot change the lifetime of raw data or output.*

### Setting Global Report Options

From the Global Report Options dialog box or Report Schedule dialog box you can set the following global options:

- **Global policy** — All raw report data can be kept indefinitely or deleted after a specified period of time. If you generate a lot of reports, you should choose to delete raw report data. Deleting raw data does not delete output HTML reports.
- **Header and footer format** — You can set up the graphic file and text that appear in the header and footer of all output reports. Graphic images must be 100 x 100 pixels or less and should be stored in the user icons directory in the report output directory on the Web server.
- **HTML Configuration** — Use this area to specify whether HTML output reports are kept forever or deleted after a specific period of time.



---

## Strategy for Reporting

This section contains a strategy to help new users begin reporting with Traffix Manager.

### Getting Started

One of the most beneficial features of the Report Manager is that you can use it to obtain a picture of your network's usual behavior.

The quickest report to run is the top N segments report. This report shows you the activity on your network and helps you determine whether that activity is predictable and consistent from week to week.

You can also configure device activity reports on your most important network devices to monitor significant changes.

### How Long Does it Take to Generate Reports?

Depending on the volume of traffic on your network and the period covered by a report, it may take anything from a minute to more than an hour for a report to be run and output. For example, a top N devices report, set up to determine the top 10 devices from a network containing 100,000 devices over a period in which 1 million connections were seen, could take an hour or more to run.

Therefore, scheduled reports are run overnight, to be delivered to your Web server or printer in the morning. *Ad hoc* reports can be started from the Report Manager but, according to the quantity of data being processed and the number of reports queued, they may not be output immediately.

### Tips and Hints

Due to the time that may be required to generate and output a report, you may wish to try the following:

#### **Use Graphs to Identify Key Components Quickly**

To identify unusual or interesting devices, groups or connections on your network, use the Top Objects and Top Connections graphs available from the Map. Then schedule reports on these objects and connections for longer term monitoring. See [Chapter 8, "Displaying Traffic in Graphs"](#) for more information.

#### **Use Grouping to Focus Reports**

To filter and focus the search for interesting data, group objects into meaningful views of your network. Then create reports for particular

groups, rather than for your entire network. See [“Creating and Assigning Attributes”](#) on [page 44](#) for more information.

### **Generate a top N Summary Report to Determine Objects for an Activity Report**

You can run top N reports in two modes:

- Summary mode just identifies the top N objects.
- Summary plus detail mode generates a report including detailed information for each of the top N objects. Reports run in this mode take longer to generate.

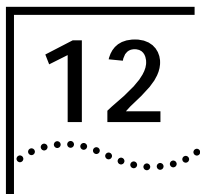
To identify key network objects, generate a top N report in summary mode. Then schedule activity reports on any objects of particular interest.

---

### **Effects of Grouping on Reports**

The creation and content of your reports is influenced in the following ways by how devices are grouped in the Map:

- The current grouping in the Map determines the groups that can be selected when configuring a report. See [Chapter 4, “Grouping Network Devices in the Map”](#) for more information about groupings.
- If you try to delete a grouping which report instances are dependent on, the reports will be displayed and you will need to delete them before you can delete the grouping.
- Editing the attributes of a particular device may cause that device to be moved into or out of a group. This affects report output if reports are being produced for any of the groups concerned.



# REPORT TYPES

This chapter describes in detail each type of report in Traffix™ Manager.

---

## Report Templates

For each kind of object — connections, devices, groups of devices, and segment — there are two types of report template, activity and top N.

### Activity Reports

Each activity report consists of two sections:

- The first section contains detailed information on the activity of each specified object.
- The second section contains information about the report itself such as its title, whether it was scheduled or run *ad hoc*, and when it was created.

### Top N Reports

Top N reports can be run in two modes:

- Summary mode just identifies the top N objects.
- Summary plus detail mode generates a report including detailed information for each of the top N objects. Reports run in this mode take longer to generate.

Each top N report consists of two or three sections:

- The first section identifies the top N objects according to one or more criteria specified by you, for example utilization and total octets.
- For a Summary plus Detail report, the second section contains a number of subsections, each comprising detailed information on an object identified in the first section.

This information is not produced for a Summary only report.

- The last section contains information about the report itself such as its title, whether it was scheduled or run *ad hoc*, and when it was created.

The different types of report are described in turn in the remainder of this chapter.

## Connection Activity Report

This report contains detailed information on each specified connection. Traffic flowing in both directions between the selected end points is used.

When selecting end points, you can select any two objects from the Map as the end points of a connection. For example:

- Device to device connection (for example, `host1` to `host2`)
- Device to group connection (for example, `server1` to `123.0.0.0` network)
- Group to group connection (for example, `US` to `UK`)
- Group to sub-group connection (for example, `US` to `Edinburgh`)

**Table 8** Connection Activity Report Charts

Report Section	Chart Title	Description
1	Connection Activity	
1.1	Protocol Distribution Of Connection By Octets	A pie chart showing the total octets within the connection, broken down by protocol.
	Protocol Distribution By Octets With Packets Overlaid	A stacked bar chart showing the total octets within the connection over the report time period, broken down by protocol. The left hand axis refers to the octet totals. The right hand axis refers to the packet totals which is shown as a line.
	Long Term Trend	A line chart showing the total octets sent and received by the device for as long as Traffic Manager has records.
	Top Conversations Within The Connection	A stacked bar chart showing the top 10 device to device conversations within the detail group, broken down by protocol.
	Long Term Trend	A line chart showing the total octets within the connection for as long as Traffic Manager has records.

(continued)

**Table 8** Connection Activity Report Charts (continued)

Report Section	Chart Title	Description
2	Report Information	Information about the report itself.

## Device Activity Report

This report contains detailed information on each specified device.

**Table 9** Device Activity Report Charts

Report Section	Chart Title	Description
1	Device Activity	
1.1	Protocol Distribution For Device By Octets	A pie chart showing the total octets sent and received by the device broken down by protocol.
	Top Conversations	A stacked bar chart showing the top 10 devices talking to the detail device by total octets sent and received, broken down by protocol.
	Protocol Distribution By Octets With Packets Overlaid	A stacked bar chart showing the total octets sent and received by the device over the report time period, broken down by protocol. The left hand axis refers to the octet totals. The right hand axis refers to the packet totals which is shown as a line.
	Long Term Trend	A line chart showing the total octets sent and received by the device for as long as Traffic Manager has records.
2	Report Information	Information about the report itself.

## Group Activity Report

This report contains detailed information on each specified group.

There are three ways you can report on groups:

- **External** — Traffic flowing into or out of the group only
- **Internal** — Traffic flowing within the group only
- **Overall** — Both external and internal traffic

**Table 10** Group Activity Report Charts

Report Section	Chart Title	Description
1	Group Activity	
1.1	Protocol Distribution Of Group By Octets	A pie chart showing the group's internal, external or overall octets broken down by protocol.
	Top Group Conversations With Protocol Distribution	A stacked bar chart showing the top 10 groups talking to the detail group by total octets sent and received, broken down by protocol. Only conversations with groups at the same level of the grouping scheme as the detail group are considered.
	Protocol Distribution By Octets With Packets Overlaid	A stacked bar chart showing the group's total internal, external or overall octets over the report time period, broken down by protocol. The left hand axis refers to the octet totals. The right hand axis refers to the packet totals which is shown as a line.
	Long Term Trend	A line chart showing the total octets sent and received by the device for as long as Traffic Manager has records.
	Top Sub-Groups With Protocol Distribution By Octets	A stacked bar chart showing the top 10 sub-groups within the detail group, broken down by protocol. The octet total has the same internal, external or overall filter as the detail group applied.
2	Report Information	Information about the report itself.

## Segment Activity Report

This report contains detailed information on each specified segment. For the purposes of reporting, it is assumed that each separate segment of your network is monitored by an agent interface.

Many sites (particularly in a switched environment) have large numbers of segments and it may be too expensive to instrument all of them with RMON-2 agents. One option at such sites is to use any existing, embedded RMON-1 only devices (hubs, switches, routers etc.) to produce lightweight Segment Activity reports for the otherwise un-instrumented segments. See [Appendix I, "Using RMON-1 Agents"](#) for more information.

**Table 11** Segment Activity Report Charts

Report Section	Chart Title	Description
1	Segment Activity	
1.1	Protocol Distribution Of Segment By Octets	A pie chart showing the top 10 protocols seen on the segment.
	Top Hosts	A stacked bar chart showing the top 10 hosts on the segment by total octets sent and received. The octets are broken down by protocol.
	Protocol Distribution By Octets With Packets Overlaid	A stacked bar chart showing the octets over the report time period broken down by protocol. The left hand axis refers to the octet totals. The right hand axis refers to the packet totals, shown as a line.
	Utilization History With Baseline	A baseline chart showing the actual utilization over the report period as a line. This is overlaid on bands representing normal, borderline and unusual utilization. These baselines are calculated using a statistical analysis of data from previous report periods. Note that baseline information does not appear immediately. You may need to generate historical data for several weeks before the baselines can be calculated.

(continued)

**Table 11** Segment Activity Report Charts (continued)

<b>Report Section</b>	<b>Chart Title</b>	<b>Description</b>
	Error History With Baseline	A baseline chart showing the actual total number of error packets over the report period as a line. This is overlaid on bands representing normal, borderline and unusual error totals. These baselines are calculated using a statistical analysis of data from previous report periods. Note that baseline information does not appear immediately. You may need to generate historical data for several weeks before the baselines can be calculated
	Generic Line Stats	A table showing counts for some generic (media independent) variables over the report period.
	Media Specific Line Stats	A table showing counts for various media specific variables. This table varies depending on the media type of the segment (Ethernet, Token Ring, FDDI).
2	Report Information	Information about the report itself.



---

## Top N Connections Report

This report calculates the top N connections by total octets sent and received over the report period.

A connection can be one of the following:

- A single conversation between two devices
- The total of multiple conversations between a device and a group
- The total of multiple conversations between two groups

You can limit the report to consider only connections between groups or devices at specified levels in the grouping, and also where each end of the connection must be within a specified parent group. Specify a high-level connection between two groups and the report tells you about the most active sub-connections it contains. For example, if you select U.S. to U.K. as your high-level connection in a geographical grouping, and select “City level” to report on, the report tells you the top city to city connections contained within the U.S. to U.K. connection.

There are lots of ways to use the top N connections report. Use the *Level* options to specify how the connections should be broken down at each end. Typically, you may want the connection to be broken down at the same level at each end.

If you are interested in the top N connections between actual devices, choose one of the following options:

- If the grouping used is one that collapses redundant groups (for example, DNS), select the *Lowest* level at each end of the connection. See “[Groupings](#)” on [page 42](#) for more information.
- If the grouping used does not collapse redundant groups (for example, Type and Network), select *Device* level to display the connections between devices.

Choose a different level to aggregate the connections between many different devices.

The following are examples of reports on geographical groupings:

- “From us at *City* level to uk at *City* level” tells you the busiest city to city connection between the U.S. and U.K., such as Boston to London or New York to Edinburgh.

- “From `us` at *Country* level to `uk` at *City* level” tells you which cities in the U.K. communicated most with the U.S.
- “From `us` at *Device* level to `uk` at *Device* level” tells you the busiest connections between individual devices in the U.S. and U.K., such as `server1` to `pc-42` or `pc48` to `ukServer`.

The following are examples of reports on the default Type and Network grouping. See [Chapter 4, “Grouping Network Devices in the Map”](#) for more information about the default groupings.

- “From `123.0.0.0` at *Network* level to `ip` at *Network* level” tells you which IP networks had the busiest connections with the `123.0.0.0` network. As `123.0.0.0` is a network, the connections are not broken down within the network.
- “From `server1` at *Device* level to `123.0.0.0` at *Device* level” tells you which machines in the `123.0.0.0` network exchanged the most traffic with `server1`.

**Table 12** Top N Connections Report Charts

Report Section	Chart Title	Description
1.1	Top Connections By Octets	A stacked bar chart containing the top N connections as measured by total octets between the two end points, broken down by protocol.
	Protocol Distribution Of Top Groups	A pie chart showing the top 10 protocols seen within all of the N connections. If more than 10 protocols are seen, the remainder are grouped as <code>other</code> .
	Connection History	A multiple line chart showing the history of the total octets for each of the N connections over the report period.
2	Detail For Top Connections	
2.1	Protocol Distribution Of Connection By Octets	A pie chart showing the total octets within the connection, broken down by protocol.
	Protocol Distribution By Octets With Packets Overlaid	A stacked bar chart showing the total octets within the connection over the report time period, broken down by protocol. The left hand axis refers to the octet totals. The right hand axis refers to the packet totals which is shown as a line.

(continued)

**Table 12** Top N Connections Report Charts (continued)

Report Section	Chart Title	Description
	Long Term Trend	A line chart showing the total octets sent and received by the device for as long as Traffix™ Manager has records.
	Top Conversations Within The Connection	A stacked bar chart showing the top 10 device to device conversations within the detail group, broken down by protocol.
	Long Term Trend	A line chart showing the total octets within the connection for as long as Traffix Manager has records.
3	Report Information	Information about the report itself.

## Top N Devices Report

This report calculates the top N devices by total octets sent and received, and by the number of “hits” over the report period. You can limit the report to consider only devices within a specified group.

For example:

- Select the `Traffix` root group and the report tells you the most active machines on the entire network.
- Select the `us` group and the report tells you the most active devices in the U.S.



*Since it is possible that the top N devices identified by total octets sent are different from the top N devices identified by hits, Section 2 of this report can contain more than N device details.*

**Table 13** Top N Devices Report Charts

Report Section	Chart Title	Description
1.1	Top Devices By Octets	A stacked bar chart containing the top N devices as measured by total octets sent and received, broken down by protocol.
	Protocol Distribution Of Top Devices	A pie chart showing the top 10 protocols seen across all of the N devices. If more than 10 protocols are seen, the remainder are grouped as <code>other</code> .
	Device History	A multiple line chart showing the history of the total octets for each of the N devices over the report period.

(continued)

**Table 13** Top N Devices Report Charts (continued)

Report Section	Chart Title	Description
1.2	Top Devices By Hits	A stacked bar chart containing the top N devices as measured by total hits, broken down by protocol. A hit is a conversation of a particular protocol between the device and another device.
	Protocol Distribution Of Top Devices	A pie chart showing the top 10 protocols seen across all of the N devices. If more than 10 protocols are seen, the remainder are grouped as <code>other</code> .
	Device History	A multiple line chart showing the history of the total hits for each of the N devices over the report period.
2	Detail For Top Devices	
2.1	Protocol Distribution For Device By Octets	A pie chart showing the total octets sent and received by the device broken down by protocol.
	Top Conversations	A stacked bar chart showing the top 10 devices talking to the detail device by total octets sent and received, broken down by protocol.
	Protocol Distribution By Octets With Packets Overlaid	A stacked bar chart showing the total octets sent and received by the device over the report time period, broken down by protocol. The left hand axis refers to the octet totals. The right hand axis refers to the packet totals which is shown as a line.
	Long Term Trend	A line chart showing the total octets sent and received by the device for as long as Traffix Manager has records.
3	Report Information	Information about the report itself.

## Top N Groups Report

This report calculates the top N groups by total octets sent and received over the report period. You can limit the report to consider only groups at a specified level in the grouping scheme within a parent group.

Some examples of group reports are:

- **Geographical grouping** — Top 10 at *City* level within the `us` group shows you the most active cities in the U.S.
- **Type and Network grouping** — Top 10 at *Network* level within the `IP` group shows you the most active IP networks.
- **Type and Network grouping** — Top 10 at *Network* level within the `Traffic` root group shows you the most active networks of any type.

The information contained in the report is shown below.

**Table 14** Top N Groups Report Charts

Report Section	Chart Title	Description
1.1	Top Groups By Octets	A stacked bar chart containing the top N groups as measured by total octets in the internal, external or overall conversations, broken down by protocol.
	Protocol Distribution Of Top Groups	A pie chart showing the top 10 protocols seen across all of the N groups. If more than 10 protocols are seen, the remainder are grouped as <code>other</code> .
	Group History	A multiple line chart showing the history of the total octets for each of the N groups over the report period.
2	Detail For Top Groups	
2.1	Protocol Distribution Of Group By Octets	A pie chart showing the group's internal, external or overall octets broken down by protocol.
	Top Group Conversations With Protocol Distribution	A stacked bar chart showing the top 10 groups talking to the detail group by total octets sent and received, broken down by protocol. Only conversations with groups at the same level of the grouping scheme as the detail group are considered.
	Protocol Distribution By Octets With Packets Overlaid	A stacked bar chart showing the group's total internal, external or overall octets over the report time period, broken down by protocol. The left hand axis refers to the octet totals. The right hand axis refers to the packet totals which is shown as a line.

(continued)

**Table 14** Top N Groups Report Charts (continued)

Report Section	Chart Title	Description
	Long Term Trend	A line chart showing the total octets sent and received by the device for as long as Traffix Manager has records.
2.1	Top Sub-Groups With Protocol Distribution By Octets	A stacked bar chart showing the top 10 sub-groups within the detail group, broken down by protocol. The octet total has the same internal, external or overall filter as the detail group applied.
3	Report Information	Information about the report itself.

## Top N Segments Report

This report calculates the top N segments by utilization, and by percentage of errors.

For most networks it is sufficient to allow Traffix Manager to select automatically the top N segments by selecting *All Segments* for the top N segments report.



*Since it is possible that the top N segments identified by utilization are different from the top N segments identified by percentage of errors, Section 2 of this report can contain more than N segment details. If the high error segments are completely different from the high utilization segments, you end up with 2 x N details in the details section.*

**Table 15** Top N Segments Report Charts

Report Section	Chart Title	Description
1.1	Top Segments By Utilization	A bar chart containing the top N segments as measured by percentage utilization of bandwidth.
	Protocol Distribution Of Top Segments	A pie chart showing the top 10 protocols seen across all of the N segments. If more than 10 protocols are seen, the remainder are grouped as <code>other</code> .
	Protocol Distribution By Octets	A stacked bar chart showing the protocol breakdown of each of the N segments by octets. The order of the bars is the same as the utilization bar chart. Because utilization is not the same as octets, the bars in this chart may not always appear in descending order. For example, the utilization on a 100Mbps Ethernet segment may be quite low compared to a 10Mbps segment, but the octet count may be considerably higher.

(continued)

**Table 15** Top N Segments Report Charts (continued)

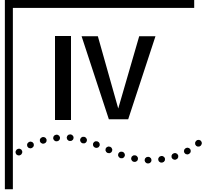
Report Section	Chart Title	Description
	Utilization History	A multiple line chart showing the history of the utilization for each of the N segments over the report period.
	Utilization Health Chart	An alternative way of viewing the utilization history. Utilization values are shown as cells with the cell color indicating the band of utilization.
1.2	Top Segments By Errors	A bar chart containing the top N segments as measured by percentage of error to total packets.
	Protocol Distribution Of Top Segments	A pie chart showing the top 10 protocols seen across all of the N segments. If more than 10 protocols are seen, the remainder are grouped as <i>other</i> .
	Protocol Distribution By Octets	A stacked bar chart showing the protocol breakdown of each of the N segments by octets. The order of the bars is the same as the errors bar chart. Because errors are not the same as octets, the bars in this chart may not always appear in descending order. For example, the errors on a 10Mbps Ethernet segment may be higher than those on a 100Mbps segment but the octet count on the 100Mbps segment may be considerably higher.
	Error History	A multiple line chart showing the history of the errors for each of the N segments over the report period.
	Error Health Chart	An alternative way of viewing the error history. Error values are shown as cells with the cell color indicating the error percentage.
2	Detail For Top Segments	
2.1	Protocol Distribution Of Segment By Octets	A pie chart showing the top 10 protocols seen on the segment.
	Top Hosts	A stacked bar chart showing the top 10 hosts on the segment by total octets sent and received. The octets are broken down by protocol.
	Protocol Distribution By Octets With Packets Overlaid	A stacked bar chart showing the octets over the report time period broken down by protocol. The left hand axis refers to the octet totals. The right hand axis refers to the packet totals, shown as a line.

(continued)

**Table 15** Top N Segments Report Charts (continued)

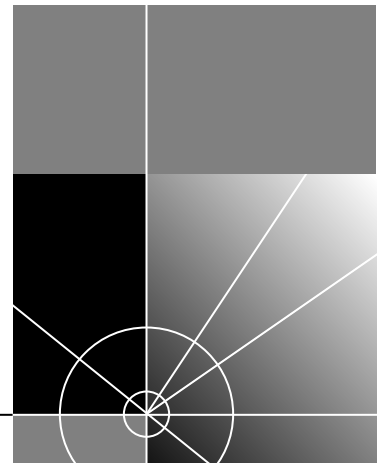
<b>Report Section</b>	<b>Chart Title</b>	<b>Description</b>
	Utilization History With Baseline	A baseline chart showing the actual utilization over the report period as a line. This is overlaid on bands representing normal, borderline and unusual utilization. These baselines are calculated using a statistical analysis of data from previous report periods. Note that baseline information does not appear immediately. You may need to generate historical data for several weeks before the baselines can be calculated.
	Error History With Baseline	A baseline chart showing the actual total number of error packets over the report period as a line. This is overlaid on bands representing normal, borderline and unusual error totals. These baselines are calculated using a statistical analysis of data from previous report periods. Note that baseline information does not appear immediately. You may need to generate historical data for several weeks before the baselines can be calculated.
	Generic Line Stats	A table showing counts for some generic (media independent) variables over the report period.
	Media Specific Line Stats	A table showing counts for various media specific variables. This table varies depending on the media type of the segment (Ethernet, Token Ring, FDDI).
3	Report Information	Information about the report itself.



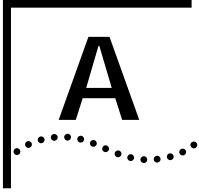


# APPENDICES AND INDEX

- [Appendix A](#) [Troubleshooting Traffic Manager](#)
  - [Appendix B](#) [Database Management Using Traffic Control Panel](#)
  - [Appendix C](#) [Aggregating Devices](#)
  - [Appendix D](#) [Using the SubnetsDB File](#)
  - [Appendix E](#) [Automatic Attribute Assignment](#)
  - [Appendix F](#) [Supported RMON-2 Devices](#)
  - [Appendix G](#) [Configuring 3Com Standalone RMON-2 Agents](#)
  - [Appendix H](#) [DHCP](#)
  - [Appendix I](#) [TFTP Server](#)
  - [Appendix J](#) [RMON and SNMP Tables Retrieval](#)
  - [Appendix K](#) [Technical Support](#)
- [Glossary](#)
- [Index](#)







# TROUBLESHOOTING TRAFFIX MANAGER

This appendix is divided into two sections:

- [Troubleshooting Traffic Manager](#)
- [Troubleshooting Reports](#)



*For information on reporting problems to 3Com, see [Appendix K, "Technical Support"](#).*

---

## Troubleshooting Traffic Manager

[Table 16](#) contains descriptions of problems you might encounter when running Traffic Manager™, and their solutions.

**Table 16** Diagnosing Traffic Manager Problems

Problem	Cause	Solution
Client Will Not Start.	Traffic server is not running.	Use the Traffic Control Panel to check that the Traffic server is running. If not, start it from the Traffic Control Panel.
	Traffic server is running in a different broadcast domain to the client.	On the machine running the client: <ul style="list-style-type: none"><li>■ Set the OSAGENT_ADDR environment variable to the IP address of the server (as a system environment variable).</li><li>■ Restart the machine.</li><li>■ Launch the client again.</li></ul>

---

(continued)

**Table 16** Diagnosing Traffic Manager Problems (continued)

Problem	Cause	Solution
No Data in the Map.		<p>Check the following:</p> <ul style="list-style-type: none"> <li>■ that you have selected an appropriate time range in the Load Traffic dialog box.</li> <li>■ one or more interfaces must be enabled in the Configure Agents dialog box. See <a href="#">Chapter 6, “Configuring Agents for Data Collection”</a>.</li> <li>■ any collector error events in the Event Log. See <a href="#">Chapter 10, “Viewing Events”</a>.</li> <li>■ that agents are responding (using the Agent Maintenance dialog box).</li> </ul>
Event Rule does not generate any events.		Check the event rule thresholds. See <a href="#">Chapter 9, “Using Event Rules”</a> . Note that events are only run once every hour and that historic event rules can take up to a day, depending on how they are configured.
When you manually enter the IP address of an agent you want to collect data from, and start collection, you get a series of collection error messages in the Event List.	Agent does not support RMON-1 or RMON-2.	<p>Consult your agent vendor’s documentation to find out if the agent supports RMON.</p> <p>If the agent does not support RMON-1 or RMON-2, Traffic Manager will not process or display collected network traffic data.</p>
When you manually enter the IP address of an agent you want to collect data from, no interfaces appear in the Configure Agents dialog box.	Agent does not have any interfaces of the supported types. See <a href="#">Appendix E, “Supported RMON-2 Devices”</a> .	<p>Consult your agent vendor’s documentation to find out if the agent supports RMON.</p> <p>If the agent does not support RMON-1 or RMON-2, Traffic Manager will not process or display collected network traffic data.</p>

## Troubleshooting Reports

See [Chapter 11, “Overview of Reporting”](#) for information on the reporting features of Traffic Manager.

## Diagnosing Reporting Problems

[Table 17](#) contains descriptions of problems you might encounter when using the reporting tools in Traffic Manager, and their solutions.

**Table 17** Diagnosing Reporting Problems

Problem	Cause	Solution
Raw report fails when running <i>ad hoc</i> or scheduled reports.	Database directory is full (raw report data is stored in the database).	<ul style="list-style-type: none"> <li>■ Increase the disk space available to the database.</li> <li>■ Delete unused raw report data to reduce the database space used for storing this report data.</li> </ul>
HTML output fails even though raw data is generated successfully.	HTML output directory is not writable.	<p>For information on why it failed, select the HTML entry and click <i>Report Info...</i></p> <p>Check that the HTML directory specified in the Traffix Control Panel has correct permissions. Note that the Traffix Control Panel can only be run directly on the server.</p>
	HTML directory has insufficient space.	Check the disk space available and allocate more space if required.
When viewing reports, message <code>Browser launched</code> is displayed but browser does not appear.	<p>On non-Windows platforms, the cause is likely to be that your path does not contain a browser.</p> <p>On Windows platforms, the cause is likely to be that HTML file types are not set up properly. Refer to your Windows documentation.</p>	<p>If <code>Browser is not in your path</code> message is displayed:</p> <ul style="list-style-type: none"> <li>■ Exit the Traffix Manager client.</li> <li>■ Update path to include Browser.</li> <li>■ Restart Traffix Manager client.</li> </ul>
Viewing reports takes very long time or never completes.	If you selected a raw data entry for which no HTML report exists, Traffix Manager must create HTML output before displaying it in a browser.	Schedule HTML output to happen following raw data generation.
	There is a backlog of reports requiring output to be generated.	Check the Report Manager to see which report is currently running. See " <a href="#">Monitoring Report Generation and Output</a> " on <a href="#">page 96</a> .
Web browser cannot find HTML file for report.	HTML files were moved or deleted outside Traffix Manager, so your Web browser cannot locate files.	<p>Always delete HTML output from the Report Manager. Do not move or delete reports outside Traffix Manager if you want to view them using Traffix Manager.</p> <p>If you inadvertently move or delete HTML output and you still have the raw report data, delete the HTML entry and use <i>Output Now...</i> to regenerate it.</p>

(continued)

**Table 17** Diagnosing Reporting Problems (continued)

Problem	Cause	Solution
Reports take very long time to run.	Reports using large amounts of data can take some time to complete.	<ul style="list-style-type: none"> <li>■ Speed up <i>ad hoc</i> report generation by generating reports for fewer numbers of devices, groups, protocols or segments.</li> <li>■ Schedule reports to run overnight rather than running <i>ad hoc</i> reports.</li> <li>■ Use the graphing tools provided from the main window to get information quickly. The main window is more suitable for real-time analysis of data. See <a href="#">Chapter 8, “Displaying Traffic in Graphs”</a>.</li> <li>■ Reduce the number of devices in the Map using the Aggregator. See <a href="#">Appendix C, “Aggregating Devices”</a>.</li> <li>■ Activity reports run more quickly than Top N reports. If you have established a set of devices or groups which you are particularly interested in, create an activity report which covers just those devices or groups.</li> </ul>
Scheduled reports do not run.	Traffix Manager processes are not running.	<p>Run the Traffix Control Panel to check the status of the Traffix Service. If the Traffix Service is not running, start it.</p> <p>Note that the Traffix Control Panel can only be run directly on the server.</p>
<i>Ad hoc</i> reports appear as <code>pending</code> but never run.	The reporting processes are busy generating another report.	<p>The reporting processes will not start generating <i>ad hoc</i> reports until the report they are currently generating is complete. If there is a queue of reports waiting to be run, it may take some time before the <i>ad hoc</i> report is run. Use the Report Manager to see which report is currently running.</p> <p>You do not need to keep the Run Now progress window open. You can request several <i>ad hoc</i> reports at one time and leave them running overnight. Use the Report Manager and output queue to see when your report is complete.</p> <p>See <a href="#">“Monitoring Report Generation and Output”</a> on <a href="#">page 96</a>.</p>
HTML files are not deleted.	Report Manager is busy running reports.	The Report Manager does not delete reports while busy running other reports. When the running reports are complete, the HTML files will be removed.
Reports do not contain as much data as expected.	Protocol filter was enabled on report.	Check if you set up protocol filtering on the report.
	Internal traffic selected.	Some reports have <code>Internal</code> , <code>External</code> and <code>Overall</code> traffic options. You are unlikely to see any <code>Internal</code> traffic on any network except your own.
	DNS layer selected for connection report is too deep to match any traffic.	In a connection report, you may have selected a DNS layer which is too deep to match any of the conversations that would otherwise contribute to the report. This type of problem may also occur with other grouping schemes. Read the generated title of the connection report carefully to check that it is sensible.

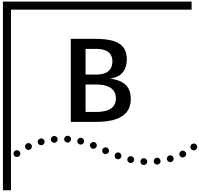
(continued)

**Table 17** Diagnosing Reporting Problems (continued)

Problem	Cause	Solution
"ERROR could not open output file: <filename>" in event viewer.	The reporter was unable to create an output file.	This is most often caused by insufficient permissions — you do not have permission to create output files where requested.







# DATABASE MANAGEMENT USING TRAFFIX CONTROL PANEL

This appendix contains:

- [Overview of Traffic Control Panel](#)
- [Overview of Database Applications](#)
- [Upgrading Traffic Manager 2.0](#)

---

## Overview of Traffic Control Panel

From the Traffic Control Panel, you can manage the operation of the Traffic™ Server, and the setup and maintenance of the data collected. Traffic Manager uses a database to store topology, trend data, collector configurations, device attributes, scheduled report templates and report data.

The latest version of the Transcend Traffic Manager Database Schema document is available at

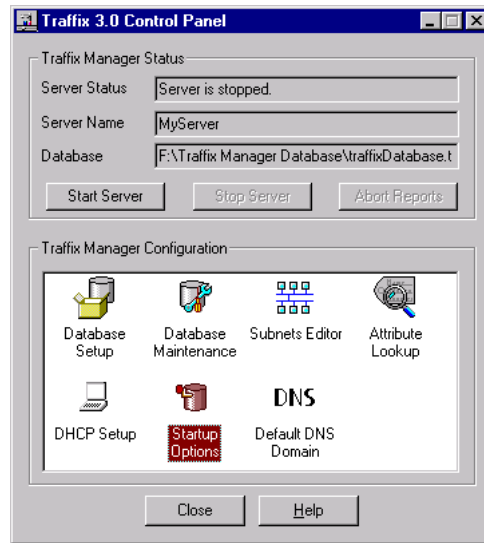
<http://support.3com.com/infodeli/tools/netmgt/traffic/family.htm>



*If you choose to use the Database Schema documentation to configure your Traffic Manager database, 3Com® can only provide limited support regarding any issues with the Traffic Manager database that occur as a result of your actions.*

*3Com strongly recommends that you do not customize or directly access the Traffic Manager database. You should only manipulate or repair the Traffic Manager 3.0 database through the Control Panel. If you choose to use the Database Schema documentation to configure your Traffic Manager database, you must fully agree to take the risk of database corruption and all support-related issues.*

A number of applications are provided in the Traffic Control Panel.

**Figure 18** Traffix Control Panel

These applications help you to manage and organize a number of databases, for example, if you want to keep extra databases for backup purposes or to provide snap shots of your network or portions of your network over time.

---

## Overview of Database Applications

The Traffix Manager Configuration panel in the Traffix Control Panel provides the following applications for managing databases.

Refer to the online help for detailed information about the functions of each application.

**Database Setup** Allows you to manage the Traffix Manager databases.

In this dialog box, you can view the following:

- The status of the Traffix Server.
- The location of the database which the Traffix Server is writing data to.
- The current size of the database. You can allocate more disk space from the Database Maintenance dialog box.

- The amount of free disk space remaining on your PC for data collection to the database.
- The location of HTML reports.

From this dialog box, you can launch the following operations:

- Create a new database to write data from the network to.



*Unless you want to get rid of the contents of a database entirely, you should always use the Clean Database application instead of deleting a database and creating a new one.*

You may already have a valid Traffic Manager 3.0 database and want to purge it of data while *preserving* discovered agents, topology information, user-assigned attributes, event rules and report instances. See [“Clean databases”](#) on [page 124](#) for more information.

- Select an existing database (other than the database currently in use) as the current database.
- Copy, delete and move databases.



**CAUTION:** *You should never move or copy a database using ordinary file operations; for example, Windows NT Explorer. You should use the Move Database and Copy Database features from the Traffic Control Panel instead.*

- Change the location of the current destination of HTML reports.
- Import Database. You can import a database that has been created by either Traffic Manager 2.0 NT or the dbexport utility in Traffic Manager 2.0 (NT and UNIX).

## Database Maintenance

In this dialog box, you can view the following:

- The status of the Traffic Server.
- The location of the database which the Traffic Server is writing data to.
- The current size of the Traffic Manager database. Data from the Collector, Reporter and Event List is stored in this database. You can specify the maximum amount of disk space which is used to store this data in this dialog box.
- The amount of free disk space remaining on your PC for data collection to the database.

- The amount of hourly and daily data which has already been collected. In this dialog box, you can specify the maximum amount of data that you want the Traffic Manager databases to hold altogether.

You can carry out the following operations from the Database Maintenance dialog box:

### Clean databases

Clean the current Traffic Manager database by selecting from the following options:

- Delete all topology information. If you choose to delete topology information, all connection data, all reports and all events are deleted also.
- Delete report instances, raw reports and HTML reports. See [Chapter 11, “Overview of Reporting”](#) for an explanation of these terms.
- Delete event rules and generated events. See [Chapter 9, “Using Event Rules”](#).

When you clean a database, the agent configurations and local DNS domains are not deleted. When you then start running against the newly-cleaned database you will not see the startup wizard again, as the agents and local DNS domains have already been configured from before the clean.

In addition, after cleaning a database, collection is suspended for the configured agents, so in order to start collecting data you have to turn off the Suspend Collection option from the Configure Agents dialog box. If you do want to use the startup wizard to reconfigure Traffic Manager, you have to create a new database.

### Repair databases

Certain types of corruption in your database can be detected and repaired. If your Traffic Manager database becomes corrupt (for example, if the machine is powered off when data is being written to the database), Traffic Manager warns you and advises you to try using the Repair Database utility.



*If the database is still corrupt after using Repair Database, you will have to revert to a backup of your database.*

3Com recommends that you back up your database regularly, the frequency depending on how important your trend data is to the way you monitor your network. If you want to view and report on your weekly data, you should back up your database once a week. If viewing and storing your trend data is less important, backing up your database once a month may be adequate.

To back up your database:

- 1 Stop the Traffix Server. See [“Stopping Traffix Manager”](#) on [page 28](#).
- 2 Copy your Traffix Manager database, using the Traffix Control Panel.
- 3 Restart the Traffix Server. See [“Launching the Traffix Manager Server”](#) on [page 26](#).
- 4 You can then make a backup of the copy, while Traffix Manager can continue to collect and store data in the “live” version.

### **Optimize databases**

Optimize re-organizes the physical location of parts of the database so that the database can be accessed more efficiently. It therefore works in an similar way to the defragmentation utility in the Windows operating system.

**Subnets Editor** Allows you to group the devices on your network by subnet, and assign default DNS domains, using the SubnetsDB file. See [“Using the SubnetsDB File”](#) on [page 133](#).

**Attribute Lookup** Allows you to configure the user-defined attribute lookup programs. See [“Contents of the User-defined Attributes Configuration File”](#) on [page 138](#) for more information.

**DHCP Setup** Controls the way that IP and MAC address mappings are obtained for Windows DHCP devices.  
See [Appendix H, “DHCP”](#), for more information.

**Startup Options** Allows you to change the name of the Traffix Server. If you are running more than one copy of Traffix Manager, you will have more than one server running in the same network. Defining a server name allows you to differentiate between Traffix Servers when multiple servers are in use.

This dialog box also allows you to select whether Traffic Manager starts automatically every time you log on to your machine.

### Default DNS Domain

Allows you to set a default *DNS domain*, if you wish to change the previously configured default. You can specify a default domain to be used for devices discovered on your local network when the DNS lookup does not return fully-qualified local names.

For example, if the default DNS domain is `acme.com` and a device resolves as `fred`, it will be given the DNS name `fred.acme.com`. This can be useful when using the DNS grouping. See [Chapter 4, “Grouping Network Devices in the Map”](#) for more information.

---

## Upgrading Traffic Manager 2.0



*Traffic Manager version 3.0 and Traffic Manager version 2.0 for NT cannot be installed on the same system. Before you can install Traffic Manager 3.0, you must deinstall Traffic Manager 2.0.*

This section describes the actions you must complete before attempting to deinstall Traffic Manager 2.0. It then describes the process for de-installing Traffic Manager 2.0. The de-installation process is divided into two steps:

- Deinstalling Traffic Manager 2.0.
- Deleting the *Transcend Traffic Manager 2.0* and *XVision* program groups and *Start* menu entries.

### Before Deinstalling

Before deinstalling Traffic Manager, ensure you complete the following steps:

- Take a backup of any files you wish to keep. For example, you may wish to keep a copy of the directory which contains all the data you have collected. You may also wish to keep a copy of the directory which contains Traffic Manager configuration files — the `SubnetsDB` file and the `AttlookupDB` file. You can find these files in `<install>\traffic\config`.
- Save any attribute lookup programs that you have written. See [Appendix E, “Automatic Attribute Assignment”](#) for more information.

## Deinstalling Traffix Manager 2.0

To deinstall Traffix Manager 2.0 for NT:

- 1 Close Traffix Manager and all related processes.  
To check which processes are running, right-click the Windows NT Taskbar and select *Task Manager*. The *Applications* and *Processes* tabs contain a list of any active programs.
- 2 From the *Start* menu, select *Settings > Traffix Control Panel* to open the Traffix Control Panel.
- 3 Double-click *Add/Remove Programs* to open the Add/Remove Programs Properties dialog box.
- 4 In the list of programs that may be deinstalled, select *Transcend Traffix Manager 2.0* and click *Add/Remove...*
- 5 When prompted to confirm your selection, click *Yes* to continue with the deinstallation or *No* to abandon it.  
If you select *Yes*, all related Traffix Manager files and directories are removed. When complete, a success message is displayed. Click *OK* to exit the dialog and return to the Add/Remove Programs Properties dialog box.
- 6 In the list of programs that may be deinstalled, select *XVision* and click *Add/Remove...*
- 7 When prompted to confirm your selection, click *Yes* to continue with the deinstallation or *No* to abandon it.  
If you chose *Yes*, the Maintenance Setup dialog box is displayed. Click *Remove All* and when prompted to confirm your selection, click *Yes*. The XVision files are removed. When deinstallation is complete, select *Yes* and click *Finish* to restart your machine when prompted.
- 8 The deinstallation process does not remove the Traffix Manager database files or directory structure.



*If you do not have any other 3Com applications installed, and if you do not have any data you wish to keep in the 3COM directory, such as Traffix Manager databases, you can delete the entire 3COM directory using Windows Explorer.*

## Program Groups and Start Menu Entries

To delete the program groups and *Start* menu entries for *Traffix Manager 2.0* and *XVision*:

- 1 To display a program group, right-click *Start* and select *Open All Users*. Double-click a program entry to display the program group.
- 2 Right-click the control button in the top left corner of the Traffic Manager program group title bar.
- 3 From the drop-down menu, select *Delete*.
- 4 When prompted, confirm the deletion of this program group by clicking *Yes* or click *No* to abandon it.

If you click *Yes*:

- The Traffic Manager program group is removed and placed in your system's Recycle Bin.
- The following error message is displayed:

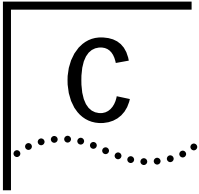
```
Start Menu\Programs\Transcend Traffic Manager NT  
v2.0 is not accessible.
```

```
This folder was moved or removed.
```

This indicates that the *Start* menu entry for Traffic Manager has been removed. Click *OK* to dismiss the message.

- 5 Repeat steps 2 to 4 for the Vision program group.





# AGGREGATING DEVICES

This appendix describes:

- [Overview](#)
- [Default Aggregation](#)

---

## Overview

Aggregation reduces the amount of memory and disk resources required by Traffic™ Manager by collating the data collected for many devices into a single device. For example, in sites where there is a lot of Internet traffic, some or all external devices can be aggregated together. This may be the only way to limit the resource usage to an acceptable level. Use the Aggregation dialog box to set up aggregation.

Once a definition has been specified and the Traffic Manager processes and Map restarted, this only affects data collected from this point on, and not data already collected.

This makes any data analysis for data which crosses an “aggregation change” boundary hard to interpret. In this case, 3Com® recommends that you start a new database. See [Appendix B](#), “Database Management Using Traffic Control Panel” for more information.

---

## Default Aggregation

Aggregation provides a solution to the problem of large numbers of devices on your network, without forcing you to discard any devices. Any loss of data prevents you from seeing a true picture of how your network is being used. Aggregation works by grouping together related devices and replacing them with a single aggregate device.

By default, all devices in the local DNS domain will be kept in detail, and it is only those outside the local domain that can be aggregated. See [“Launching the Traffic Manager Client”](#) on [page 26](#) for more information about local domains. You can specify an alternative aggregation policy.

## Specifying an Aggregation Policy

To aggregate devices on a particular network, it is necessary for the aggregator to be configured for that network. This is done by specifying an aggregation policy.

Once an aggregation policy has been configured, it only affects data collected from that point on.

An aggregation policy consists of three parts: a local domain specification, a default action and a maximum device limit.

### Local Domain Specification

As well as reducing the amount of memory and disk resources required, aggregation is also an intuitive way of specifying which devices are of interest and should therefore be monitored closely. You can specify a list of the DNS domains which will be referred to as the local domain(s). These are the domains which you want to retain at device-specific level for detailed monitoring. Any device whose resolved DNS domain matches one of these specified DNS domains, or a sub-domain of one of the specified DNS domains, is considered to be local and will be kept in detail.



*Only IP addresses can have a DNS domain, and therefore only IP addresses are considered for aggregation. Non-IP network devices are always be considered to be local, and so will be kept in detail.*

You can assign DNS domains to subnets using the SubnetsDB file. Subnets can be assigned any DNS domain, but 3Com suggests that you use local domains. If you provide a local DNS domain name for a subnet, a device in this subnet will be placed in this domain, if DNS lookup fails for the device. This ensures that such devices appear in the correct group when you use the DNS grouping.

When Traffix Manager discovers a new IP device on your network, it performs a DNS lookup for the DNS name of that device. If this lookup fails, or if your site has no DNS, Traffix Manager will check the SubnetsDB file to see if the device is in a given subnet. If so, it will assign the DNS name of the subnet to the device. If the device is not found in SubnetsDB, then a final check is done to see if it is in the same subnet as the Traffix Manager Server. If it is, the device is assigned to the subnet `home-subnet` and the DNS domain is set to that of the server (if it has one). You can override this behavior by making sure that there is an entry in the SubnetsDB file for the subnet of the Traffix Manager Server. See [“Using the SubnetsDB File”](#) on [page 133](#) for more information.

## Selecting the Default Aggregation Action

The default aggregation action is the method of aggregation applied to network devices which have a DNS name, but which are not contained within one of the local DNS domains.

There are three default aggregation actions, from which you can select and apply one to non-local DNS domains. In the following examples, it is assumed that `acme.com` is not in the Local Domain Specification.

- **Automatic** This describes the “standard” default aggregation action. Traffic Manager builds up a tree of *DNS domains* for aggregation purposes.

When aggregation becomes necessary, all devices in each of the *lowest* DNS domains will be aggregated into a single device, to represent each domain. For example, all devices in the domain `engineering.acme.com` are aggregated into a single device, representing `engineering.acme.com`.

When all domains at this lowest level have been aggregated, Traffic Manager then aggregates each domain at the next level. Following this example, `engineering.acme.com` and `office.acme.com` are both aggregated to `acme.com`.



*You cannot undo aggregation. If you add an aggregated DNS domain to a local domain, all newly discovered addresses will be mapped to the (aggregated) representative device.*

The two default aggregation actions described below provide you with control over how devices are aggregated. However, if the maximum device limit is reached and the default action is not automatic, automatic aggregation is attempted, to make room for new local devices.

- **Aggregate at DNS Layer** By selecting this option you specify a DNS layer and a direction. This direction can be either *From name*, or *From tail*.
  - *Aggregate from name* allows you to specify any layer above the name of the device.

If layer 1 above the name is selected, the device `office.acme.com` is aggregated into the device representing the DNS domain `acme.com`.

If layer 2 above the name is selected, the device `office.acme.com` is aggregated into the device representing `.com`.

If a network device does not have the selected layer above the name, then the device is aggregated into a device representing the highest DNS layer possible. `office.acme.com` does not have a layer three above its name and would therefore be aggregated into the device representing the DNS layer `.com`.

- *Aggregate from tail* allows you to specify a DNS layer above the end of the device name. A network device that has a non-local DNS domain is aggregated into a Traffix Manager device representing this DNS layer.

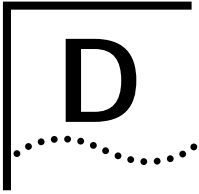
For example, if DNS layer 2 is selected, the device `mydevice.acme.com` is aggregated into the device representing the DNS domain `acme.com`.

- **Discard** Any network device that has a non-local DNS domain is discarded immediately, and no data for that device is collected.

### Setting a Maximum Device Limit

You can specify a device limit of 100,000 devices. This allows you to monitor local devices in detail, but reduce the detail of data kept about non-local devices. This setting is treated as a “hint” by Traffix Manager: if new local devices are seen after this user-defined limit is reached, the setting is increased gradually, up to the maximum version limit, to allow for the new local devices to be stored.

This prevents unnecessary loss of information about local devices.



# USING THE SUBNETSDB FILE

---

## Using the SubnetsDB File

This facility allows you to group the devices on your network by subnet. Click *Subnets Editor* in the Traffix™ Control Panel to edit the subnet definition file, which contains information about subnet groupings. This file can be edited and reapplied at any time.



- *This facility extends the basic subnetting provided by the NL attribute. See [“Predefined Attributes” on page 40](#).*
- *Subnets can only be applied to devices with IP addresses.*
- *Multicast addresses cannot be used.*
- *All addresses must be in dotted decimal format.*

To set up subnets:

- 1 Edit the `subnetsdb` file using the Subnets Editor provided in the Traffix Control Panel.
- 2 For each subnet you wish to add, you must specify the following:
  - The significant part of the subnet address
  - A subnet mask
  - The name of the group
  - The DNS domain



*Check the Event Log for errors after you have changed the SubnetsDB program. If an error occurs, the whole SubnetsDB file is ignored.*

For example, if the PCs on your network were all located within the subnet 140.6.0.0, you might add the following entry to the subnet configuration file:

<b>subnet</b>	<b>mask</b>	<b>name</b>	<b>domain</b>
140.6.0.0	255.255.0.0	Group1	3com.com

Entries can appear in any order.

Subnet masks must comply with the primary internet network class types by covering at a minimum the part of the address that represents the network bits. In [Table 18](#), \* is any number between 0 and 255.

**Table 18** Subnet Masks

Class	Description	Mask
A	<p>1 7 24 0 Network Host</p>	255.*.*.*
B	<p>1 1 14 16 1 0 Network Host</p>	255.255.*.*
C	<p>1 1 1 21 8 1 1 0 Network Host</p>	255.255.255.*

If a subnet mask spans more than one class A/B/C subnet then only the first entry should be used. For example, if the subnet is 130.99.92 and the mask is 255.255.252.0, this spans four class A/B/C subnets (130.99.92, 130.99.93, 130.99.94, and 130.99.95). However, only the first entry should be added to the file:

subnet	mask	name	domain
130.99.92	255.255.252.0	MySubnet	acme.com

When you provide a DNS domain name for a subnet, devices in this subnet will be placed in this domain, if the DNS lookup fails for a device. This ensures that these devices appear in the correct group when you use the DNS grouping.

When Traffix Manager discovers a new IP device on your network, it performs a DNS lookup for the DNS name of that device. If this lookup fails, or if your site has no DNS, Traffix Manager will check the SubnetsDB file to see if the device is in a given subnet. If so, it will assign the DNS name of the subnet to the device.

If the device is not found in SubnetsDB, then a final check is done to see if it is in the same subnet as the Traffix Server. If it is, the device is assigned to the subnet `home-subnet` and the DNS domain is set to that of the server (if it has one).

You can override this by making sure that there is an entry in the SubnetsDB file for the subnet of the Traffix Server.

- 3 When you have added the subnets you require, click *OK* in the subnet definition file editor.

Traffix Manager detects changes to the subnet definition file and reloads it automatically.

- 4 If you already have devices showing in the Map, reload the subnets attributes using the Reload Attributes dialog box, which you access from the *Edit* menu in the main window.
- 5 Create a subnets grouping. See [“Predefined Groupings”](#) on [page 43](#) for information on how to create a site-specific subnet grouping.
- 6 Apply the grouping.

### How Subnet Grouping Works

Subnet grouping works in the following way:

- The subnet address and mask are combined with a Boolean AND operation to produce a key.

For example, when the subnet address 140.6.0.0 is given the Boolean AND command with the mask 255.255.0.0 the resulting key is:

```
140.6.0.0=10001100000001100000000000000000
```

```
255.255.0.0=11111111111111110000000000000000
```

```
Result of AND=10001100000001100000000000000000
```

- To determine whether a device qualifies for a subnet, the key value is compared with the value created by ANDing the subnet mask with the device's IP address. If these values are not equal, Traffix Manager does not accept the devices as part of the subnet.

For example, Traffix Manager has detected a device with the IP address 140.7.0.6. To determine whether the device qualifies for the pc subnet, Traffix Manager does the following calculation:

```
140.7.0.6=10001100000001110000000000000110
```

```
255.255.0.0=11111111111111110000000000000000
```

```
Result of AND=10001100000001110000000000000000
```

Since the results are not equal, Traffix Manager concludes that the device is not part of the pc subnet.

- When matching subnets and devices, Traffix Manager assumes that the best match for a device is the subnet with the most set bits in the mask.

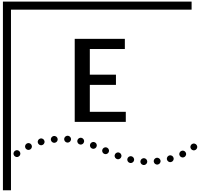
For example, if the `SubnetsDB` file was to contain the following entries with the same subnet address:

<b>subnet</b>	<b>mask</b>	<b>name</b>	<b>domain</b>
<b>89.0.0.0</b>	<b>255.0.0.0</b>	<b>Group1</b>	<b>3com.com</b>
<b>89.0.0.0</b>	<b>255.255.0.0</b>	<b>Group2</b>	<b>3com.com</b>

Any device matching both of these subnets would be placed in Group 2, as this has 16 set bits in its subnet mask, whereas Group 1 has only 8 set bits.

- If a device matches two subnets and both subnets have the same number of set bits in their masks, then Traffic Manager may assign the device to either of these groups.





# AUTOMATIC ATTRIBUTE ASSIGNMENT

This appendix describes:

- [Overview](#)
- [Contents of the User-defined Attributes Configuration File](#)
- [Performing Attribute Assignment](#)
- [Using the fileattrs Program](#)
- [Using the dblookup Program](#)
- [Writing your own program](#)

---

## Overview

Automatic attribute assignment within Traffix™ Manager lets you automatically import attribute values from various data sources to create groupings and to identify objects in the Map.

The data sources could be a text file, a Microsoft Excel spreadsheet, a Microsoft Access database or a program that you write. A program can carry out arbitrary processing, such as searching a file or performing a database lookup.



*Attributes can also be manually assigned to objects using the Attributes option (see [Chapter 4, "Grouping Network Devices in the Map"](#) for more information on attributes).*

Automatic attribute assignment is set up using the user-defined attributes configuration file.

This file can be edited by double clicking on *Attribute Lookup* in the Traffix Control Panel. The contents of the file are described in detail in ["Contents of the User-defined Attributes Configuration File"](#) on [page 138](#).

By editing the user-defined attributes configuration file, you select which programs are used to determine attributes for objects. You can use the standard programs supplied, or you can create your own custom programs.

There are two standard programs and one example program provided:

- `fileattrs` — Assigns attributes to devices automatically, based upon a configuration file containing comma-separated data which you must provide. For example, use this file to assign a MAC address to a specific network layer address. See [“Using the fileattrs Program” on page 140](#).
- `dblookup` — Assigns attributes to devices automatically, based upon the contents of a Microsoft Access database or a Microsoft Excel spreadsheet. See [“Using the dblookup Program” on page 142](#).
- `nbtlookup.exe` — An example program which uses NetBios Status messages to find out the names of users who are currently logged on to the Windows system. The first argument is the name of the subnet to which the request should be restricted (for example, home-subnet). It creates two attributes: **OS Type** and **User**. OS Type is set to *Windows* if the device responds to the NetBios message and User is set to the NetBios user name, if there is one. You could set up a grouping using the NL Type, OS Type and User attributes (in that order) to see the traffic generated by a particular PC user. The code for this example can be found in `<install dir>/examples/c/nbtlookup`.

---

### Contents of the User-defined Attributes Configuration File

This file can be viewed or edited by double clicking on *Attribute Lookup* in the Traffix Control Panel.

Each line of the file represents an attribute lookup program which is run when Traffix Manager is trying to discover attributes for a particular object. This happens when a new device is discovered, or when you use the Reload Attributes dialog box.

When Traffix Manager discovers attributes for a particular object, it runs each of the programs in the user-defined attributes configuration file in turn. By adding your own programs to this file or by removing existing entries from the file you can control how attributes for devices are determined.

**File Format** Lines beginning with # are comments and are ignored. All other lines take the form:

```
<Name> <label> <filename> <arguments> <flag>
```

- <label> is used in the collector event logs to refer your attribute lookup program. Otherwise it is unused.
- <filename> is the name of the attribute lookup program. This should normally be an executable file located in the main Traffix Manager install directory (by default this is C:\Transcend Traffix Manager). This program could be one of the standard attribute lookup programs (fileattrs or dblookup), or it could be an attribute lookup program which you have written yourself and copied to the Traffix Manager install directory. If your filename contains the space character, then surround it with double quotes (" ").
- <arguments> are the arguments to be passed to the attribute lookup program on the command line. The correct arguments to pass to fileattrs and dblookup are described in ["Using the fileattrs Program"](#) on [page 140](#) and ["Using the dblookup Program"](#) on [page 142](#). If your arguments contain the space character, then surround them with double quotes (" ").
- The <flag> column should normally be TRUE. If this column is FALSE then the attribute program in question is not used to determine attributes when devices are newly discovered; it is only run when you explicitly reload attributes from Traffix Manager using the Reload Attributes dialog box.

Note that you can add the same program to the configuration file several times with different arguments. For example, if you want to use fileattrs to lookup your own data file, you can add an entry like this:

```
Mylookup fileattrs.exe "c:\my data\data.txt" TRUE
```

You can specify up to 14 programs, and place them in any order.

The programs are activated sequentially, so if one program is dependent upon the results of another it must appear after that program in the list. As a result, you can form a chain of processes that extend attribute assignments depending upon the outcome of the previous process.

---

## Performing Attribute Assignment

Attribute assignment is carried out on any newly discovered devices. In addition, you can force a refresh at any time by using the Reload Attributes dialog box. Refer to the online help for the Reload Attributes dialog box for more information.

---

## Using the fileattrs Program

The `fileattrs` program assigns attributes to devices automatically based upon a configuration file which you provide. The source code for the `fileattrs` program is provided in one of the following directories:

- `<installdir>\TraffixServer\examples\source\c\fileattrs.`
- `<installdir>\TraffixServer\examples\source\vb\fileattrs.`
- The program itself is in `<installdir>\TraffixServer.`

## Configuration File Format

The configuration file must take the following format:

```
*KEY:<number of key fields>
*ATT:<comma separated list of attribute names>
<comma separated list of attribute values>
<comma separated list of attribute values>
```

KEY fields are those fields which should be used for matching against devices, and are the first N attributes in the attribute names list. Putting a '\*' in place of an attribute value in a comma separated list will cause a match with any attribute value.

### Configuration File Example 1

To map from DNS Layer 1 to a country, you would set KEY to be 1 as shown below:

```
*KEY:1
*ATT:DNS Layer 1, Country
com, USA
edu, USA
de, Germany
it, Italy
uk, UK
*, Somewhere else
```

## Configuration File Example 2

To assign user and operating system information to devices based upon their address:

```
*KEY:2
*ATT:NL Type, NL Address, User, O/S
IP, 104.240.20.10, Joe Bloggs, Solaris 2.5
IP, 104.240.20.8, Joe Bloggs, Windows 95
IP, 104.240.20.13, John Smith, Solaris 2.5
IP, 104.240.20.14, General Use, AIX 4.1
```

If the discovered device has the NL Type IP and an NL Address of 104.240.20.13, this matches the key fields of the third entry and assigns values to the User (John Smith) and O/S (Solaris 2.5) attributes.

## Running fileattrs

The user can have many different configuration files, each running with its own copy of `fileattrs` and so with its own entry in the user-defined attribute configuration file. The configuration file should be passed at the parameter to `fileattrs`.

For example, if two configuration files — `COUNTRY.TXT` and `MACHINEINFO.TXT` — were contained in `c:\data`, then you could add the following two lines to the user-defined attribute configuration file:

```
Country fileattrs.exe c:\data\country.txt TRUE
machineinfo fileattrs.exe c:\data\machineinfo.txt TRUE
```

Attributes would then be assigned to devices based on the contents of these two configuration files.



*If you change the contents of the configuration file, then you must restart the Traffic Manager Server for your changes to take effect. If `fileattrs` detects a syntax error in the configuration file, the Traffic Manager Server stops. You can view any error message in the Event List.*

## How fileattrs Works

When a device is discovered, `fileattrs` does the following:

- 1 It finds the `KEY` attribute(s) for that device, and sees if it matches any of the entries listed in the file. If it does, then it assigns the appropriate values for the attributes listed in `ATT` to that device.
- 2 The special attribute value `'*'` matches any attribute in the key column. If no matching entry is found in the configuration file for a particular device, no attributes are assigned.

The `KEY` attribute(s) for that device can be any of the attributes which are assigned automatically by Traffix Manager, for example, NL Address and NL Type. See “Predefined Attributes” on page 40 for a list of attributes which are automatically assigned by Traffix Manager. If you have other attribute lookup programs running, you may also use attributes which have already been assigned by these programs as `KEY` attribute(s).

---

### Using the `dblookup` Program

The `dblookup` program assigns attributes to devices automatically based upon lookup-tables stored in a database or a spreadsheet which you provide. The source code for the `dblookup` program is provided in `c:\Transcend Traffix Manager\TraffixServer\examples\vb\dblookup` while the program itself is in `<installdir>\Traffix Server`.

### Lookup Database Structure

Access/Excel lookup tables have a common structure. The information should be stored in tables named as follows, where N is a number between 1 and 10 which determines how many key attributes the lookup is based on (this is similar to the `KEY: N` line in `fileattrs`' configuration file):

- `lookup_N`: general lookup table;
- or:
- `ARP_N`: lookup table for ARP devices;
- `IP_N`: lookup table for IP devices;
- `IPX_N`: lookup table for IPX devices;
- `NetBEUI_N`: lookup table for NetBEUI devices;
- `other_N`: lookup table for other devices.

In each lookup table, the first N columns must be the key columns. In Access, set the fields order in the table so that key attributes are presented first. In Excel, the first column(s) are the key columns.

Note that there should be either one `lookup_N` table, or a set of network-type lookup tables. If there is a `lookup_N` table as well as network-type lookup tables, `dblookup` only looks up attributes from `lookup_N` and ignores any other table. Also, there should be at most one table of a given type: for example, if you create `IP_1`, `IP_3` and `IP_4` tables, then `IP_3` and `IP_4` is ignored. It is permitted to have a restricted set of

network-type lookup tables: for example, a database containing only IP\_1 and other\_2 lookup-tables is valid.

For specific information about Access or Excel lookup-tables, see below.

### Default Values

Devices may be assigned default values. If no full match was found for the current device, `dblookup` looks for default entries defined with star ('\*') as the key attribute values, and assigns the new attributes with the values of the best match (the one with as few stars as possible).

If no match is found for the current device, `dblookup` does not set any attribute, but waits for a new device to be looked-up.

[Table 19](#) shows an example of this:

**Table 19** lookup\_2

lookup_2		
NL Type	DNS Layer 1	Country
IP	Fr	France
IP	Uk	U.K.
IP	De	Germany
IP	*	<unknown>
*	*	<?>

- `lookup_2` is a general lookup table based on 2 attributes: NL Layer Type and DNS Layer 1. This lookup table sets the value for the Country attribute.
- An IP device called 'www.demon.co.uk' gets the 'U.K.' Country attribute;
- An IP device called 'www.yahoo.com' gets the '<unknown>' Country attribute;
- An IPX device gets the '<?>' Country attribute.

### Access Database

The lookup-tables should be either standard Access tables or queries; the column names must match Traffix Manager attribute names. You can improve performance by defining indexes on the key columns.

**Excel Worksheet** The lookup-tables are stored in Excel named-ranges. Lookup named-ranges can be stored on separate worksheets or in the same worksheet. To create a named-range, simply select the cells containing your data, select *Insert/Name/Define* from the menu, supply a name for your range and click *Add*. The worksheet can contain any other information you want and this does not interfere with the lookup.

The range's name must be the lookup-table name (IP\_1 for example) and the first row consists of Traffix Manager attribute names. `dblookup` looks for named-ranges first, before looking for lookup worksheets.

**Excel Workbook** The lookup-tables are stored in Excel workbooks on a one-table-per-worksheet basis. In this case, the worksheet name must be the lookup-table name (IP\_1 for example) and the first row consists of Traffix Manager attribute names. The worksheet may not contain any other information apart from your lookup-data.

**Running dblookup** The user can have many different lookup databases, each running with its own copy of `dblookup` and so with its own entry in the user-defined attribute configuration file. The database location should be passed to `dblookup` as its first parameter.

For example, if two lookup databases `companies.mdb` (Access database) and `continents.xls` (Excel workbook) were contained in `c:\data`, then you could add the following two lines to the user-defined attribute configuration file:

```
Companies dblookup.exe c:\data\companies.mdb TRUE
Continents dblookup.exe c:\data\continents.xls TRUE
```

Attributes would then be assigned to devices based on the contents of these two databases.



*If you change the contents of the configuration file, then you must restart the Traffix Manager Server for your changes to take effect.*

Lookup databases may be modified 'on the fly': the `dblookup` program always uses the most recent data from the database, and does not need be restarted when the data was changed.

**How dblookup Works** `dblookup` tries to open the database provided on its command line, then looks for the lookup tables.



Then, when a device is discovered, `dblookup` does the following:

- 1 `dblookup` builds a SQL string with the device's key attributes values and runs a query against the database to find a match.
- 2 If no match is found, it waits for the next device.
- 3 Otherwise it takes the best match, that is to say the one with as few stars as possible.
- 4 If two full matches are returned, `dblookup` logs an error; otherwise, it takes the result of the first partial match encountered.

---

## Writing your own program

If the standard attribute lookup programs `fileattrs` and `dblookup` are not sufficient for your requirements, you can write your own attribute lookup program.



*In order to write your own user-defined attribute program, you need Microsoft Visual C++ V5.0 or later, Microsoft Visual Basic or another tool which allows you to compile a program. The rest of this section assumes you are familiar with programming either C or Visual Basic.*

All example programs are included in  
`<installdir>\TraffixServer\examples`.

### Structure of an Attribute Lookup Program

Every time Traffix Manager wants to find out attributes for a device, it calls all the attribute lookup programs in the user-defined attribute lookup configuration file (see "[Contents of the User-defined Attributes Configuration File](#)" on [page 138](#)) and asks them to provide attributes for the device.

When you write your own attribute lookup program, your program has to respond to these requests from Traffix Manager and supply attributes for a particular device. Communication with Traffix Manager is done using the functions in the `attripc.dll` library which is in `<installdir>\TraffixServer`. Even if you do not know much about DLLs, these functions are designed to make writing your own attribute lookup program as simple as possible.

The main three functions provided by the `attripc.dll` library are `GetNextLookup()`, `GetAttribute()` and `SetAttribute()`. Below is an example of the central loop of a simple attribute lookup program

(there is one version in Visual Basic and one in C):

**Figure 19** Simple attribute lookup process in C

```
while ( GetNextLookup() )  
  
{  
    if ( strcmp( GetAttribute( "NL Type" ), "IP" ) == 0 )  
        SetAttribute( "New Device", "TRUE" );  
}  
}
```

**Figure 20** Simple attribute lookup process in Visual Basic

```
While GetNextLookup <> 0  
  
    If GetAttribute "NL Type" = "IP" Then  
        SetAttribute "New Device", "TRUE"  
    End If  
  
Wend
```

The idea behind this program is that every newly discovered IP device on the network is assigned a value of TRUE for the New Device attribute. You could use this attribute assignment to group together all the newly discovered devices on your network with the Map.

This shows the fundamental structure of any attribute lookup program:

- Calling the `GetNextLookup` function causes your program to wait until Traffix Manager wants your program to lookup another attribute, or until Traffix Manager exits. The function returns the value 1 if there is a device whose attributes should be looked up, or 0 if it wants your program to exit.
- When `GetNextLookup` returns 1, Traffix Manager expects the program to determine attributes for one device. The `GetAttribute` function can be used to discover the value of any attribute for the device, and the `SetAttribute` function can be used to set an attribute assignment.
- In this program, for each device, the program checks the value of the `NLType` using `GetAttribute`. If this attribute is set to IP, then it sets

an attribute `New Device` to the value `TRUE`. `NL Type` is a built-in attribute which is always set to the network type of a device. This means that every IP device is assigned the attribute `New Device` with a value of `TRUE`.

- Because of the while loop in the program, the program keeps assigning attributes for devices until Traffix Manager is finished with it.

By replacing this simple loop with your own code, you can write a program which assigns your own attributes to devices using your own algorithm.

`GetAttribute` returns the value of any attribute which has already been assigned, for example, `NL Address` and `NL Type`. See “Predefined Attributes” on page 40 for a list of attributes which are automatically assigned by Traffix Manager. If you have other attribute lookup programs running, you may also use `GetAttribute` to get an attribute value assigned by another program.

## Writing and Building Your Own Attribute Lookup Program

To build your own attribute lookup program, you should copy one of the example programs and modify it. You can also look at these programs for more examples of how to write attribute lookup programs. There are 6 example programs supplied, as shown in [Table 20](#).

**Table 20** Example Programs

Name	Language	Description
<code>fileattrs</code>	C	Complex program which parses a text file and uses it to assign attributes (see “ <a href="#">Using the fileattrs Program</a> ” on <a href="#">page 140</a> ).
<code>nbtlookup</code>	C	Example program which uses NetBios Status messages to find out the names of users who are currently logged on to the Windows system.
<code>country</code>	C	Simple example program which assigns an attribute <code>country</code> based on DNS name.
<code>template</code>	C	Empty attribute program which does nothing, but which contains all the necessary project files, source files and include files to build an attribute lookup program.
<code>dblookup</code>	Visual Basic	Complex program which assigns attributes based on the contents of a spreadsheet or database (see “ <a href="#">Using the dblookup Program</a> ” on <a href="#">page 142</a> ).

(continued)

**Table 20** Example Programs (continued)

Name	Language	Description
country	Visual Basic	Simple example program which assigns an attribute country based on DNS name.
template	Visual Basic	Empty attribute program which does nothing, but which contains all the necessary project files and declarations to build an attribute lookup program.

The C examples are located in `C:\Transcend Traffic Manager\TrafficServer\examples\c` and the Visual Basic examples are in `C:\Transcend Traffic Manager\TrafficServer\examples\vb`. You should copy one of these samples to your own directory before modifying it.

Attribute lookup programs must be able to find the `attripc.dll` file when they are running. This file is located in the Traffic Manager install directory. In order that your program can find this file, you should copy your program to the Traffic Manager install directory and run it from there, or you should add the Traffic Manager install directory to the PATH environment variable (it must be added as a system environment variable, not a user variable). Be careful not to overwrite any of the executables already in the Traffic Manager install directory.

Once you have built your attribute lookup program and copied it if necessary, you should add it to the user-defined attribute program configuration file (see [“Contents of the User-defined Attributes Configuration File”](#) on [page 138](#)).

### Library functions available

[Table 21](#) shows a full list of the functions available to attribute lookup programs in the `attripc` DLL library:

**Table 21** Functions available to lookup programs in the `attripc` DLL library

Function	Description
<code>GetNextLookup</code>	Takes no arguments. Returns an integer. This function waits until Traffic Manager wants to determine new attributes for a device, or until Traffic Manager is closing down. If Traffic Manager wants to determine attributes for a device, this returns 1. If Traffic Manager wants your program to exit, this function returns 0.

(continued)

**Table 21** Functions available to lookup programs in the attripc DLL library

Function	Description
GetAttribute	Should be called sometime after GetNextLookup. Takes an attribute name as an argument. Returns the currently assigned value of that attribute for the current device as a string. Returns an empty string if the specified attribute is not assigned.
SetAttribute	Should be called sometime after GetNextLookup. Takes an attribute name and an attribute value as arguments. Assigns the specified attribute value for the current device.
IsAttributeSet	Should be called sometime after GetNextLookup. Takes an attribute name as an argument. Returns an integer/Boolean. Returns 1/True if the named attribute is currently assigned for the current device and 0/False if the named attribute is not currently assigned for the current device.
LogError, LogInfo	These functions take a string as an argument. The string is logged to the Traffix Manager Event List directory, such that it can be viewed in the Traffix Manager Event List. LogError logs an error message, while LogInfo logs a normal informational message.

Other points to note about user-defined attribute lookup programs:

- If your program exits prematurely, for example, it crashes, then the Traffix Service stops. Therefore you must ensure that your program is reliable.
- Your program must startup within 30 seconds. This means that your program must call `GetNextLookup` within 30 seconds. If 30 seconds is not long enough for your program, then you can control this time-out by setting a system environment variable `TFX_ATTRSTART_TIME` to a number of seconds, for example, 60. Once your machine has been rebooted, this new time-out takes effect.
- Your program must complete the lookup of attributes for a device within 30 seconds. After 30 seconds any attribute values your program assigns are ignored. Note that this time-out can also be controlled by setting a system environment variable `TFX_ATTRLOOK_TIME` to a number of seconds. Once your machine has been rebooted this new time-out takes effect.

### Testing Attribute Lookup Programs

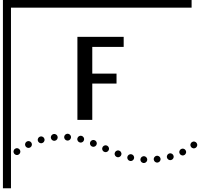
If you want to test your attribute lookup program or test a data file for one of the standard attribute lookup programs before adding it to the user-defined attribute program configuration file, there is a very simple utility provided which allows you to do this. This utility can only test

attribute lookup programs which depend on the Name, NL Type, NL Address, Network or DNS attributes.

Run the program `AttrLooktest.exe` in `<installdir>TraffixServer` (this is not on the Windows *Start* Menu). The program displays a dialog box which allows you to run an attribute lookup program, providing command-line parameters if necessary. Thus you can run your own program, or you can run one of the standard programs (`dblookup` or `fileattrs`) providing your datafile as an argument. (Note that the user-defined attribute program configuration file is not used.)

If your program is working properly, then a dialog box appears which allows you lookup attributes for any device you choose. Set the Name, NL Type, NL Address, and Network controls on the dialog to appropriate values for some device and then click *Lookup*. The list on the right of the dialog box shows the attributes returned by your lookup program. The program does not check that the attributes which you enter make sense.

The program only passes the attributes Name, NL Type, NL Address, and Network to your program. If you choose *IP* as the NL Type then the program simulates DNS attributes by breaking up the Name attribute which you have entered.



# SUPPORTED RMON-2 DEVICES

---

## 3Com Agents

The current list of 3Com agents is available from the 3Com web site:  
[http://www.3com.com/network\\_management/probe\\_interop](http://www.3com.com/network_management/probe_interop)



*Using Firmware version 4.17, the agents support all RMON-1 and RMON-2 groups. Version 4.10 or later is needed on the single port and dual port agents for Y2K compatibility.*

---

## Supported Interface Types

Traffix™ Manager supports agents with the following interface types:

**Table 22** Supported Interface Types

Interface Type	MIB2 ifType	Supported on RMON-1 / RMON-2 Compliant Agents
Ethernet	6	Both
ISO 8802.3	7	Both
Token Ring	9	Both
FDDI	15	RMON-2 only
Point-to-Point Serial	22	RMON-2 only
Frame Relay	32	RMON-2 only
AAL5 (ATM)	49	RMON-2 only
Fast Ethernet	62	Both
Fast Ethernet FX	69	Both
X25	5	RMON-2 only
PPP	23	RMON-2 only
Proprietary Virtual	53	RMON-2 only







# CONFIGURING 3COM STANDALONE RMON-2 AGENTS

This appendix contains the following sections:

- [Downloading Firmware to 3Com Standalone Agents](#)
- [Setting the Operational Mode on 3Com Standalone RMON-2 Agents](#)

---

## Downloading Firmware to 3Com Standalone Agents

You should always run the latest version of management software (*firmware*) in the agents on your network. Running the most up-to-date version of agent firmware has the following benefits:

- The latest release includes all bug fixes from previous versions.
- For full RMON-2 functionality you must have the latest version of firmware installed. Firmware releases prior to version 4.17 are incompatible with Traffix™ Manager 3.0.

Firmware files are stored on the machine where the Traffix Server is installed. When you install the Traffix Server, you automatically install the TFTP server on the same machine.

For instructions on how to download the latest version of firmware, refer to the Firmware Upgrade documentation that ships with Traffix Manager.

Before you can download agent firmware, you must launch the TFTP server, as it serves out all firmware files. Network devices can log in and download files from the TFTP server. The agents on your network must therefore be able to access the machine where the TFTP server is installed.

You launch the TFTP server by clicking *Programs* on the *Start* menu, and then selecting *Transcend Traffix Manager v3.0 TFTP Server* from the *Transcend Traffix Manager* menu.

For known issues with the TFTP Server, see the Traffix Manager Release Notes that are shipped with this product.



**CAUTION:** Downloading firmware to an agent causes the agent to cold restart. Refer to the *Firmware Upgrade documentation* or your agent documentation for a description of the data lost when an agent is cold restarted. The latest version of the *Firmware Upgrade documentation* is available from the 3Com web site:

<http://www.support.3com.com/infodeli/tools/netmgt/rmonprob/family.htm>.

## Setting the Operational Mode on 3Com Standalone RMON-2 Agents

The current mode of the agent is displayed in the Agent Hardware Maintenance dialog box. 3Com recommends that you use the *RMON-2 Traffic Mode*, because this sets tables on an agent to an appropriate size for use with Traffic Manager.

As some tables created by Traffic Manager can be very large, including RMON-2 addressMap and matrixTopN, other tables' memory sizes are decreased to make the best use of the agent's resources (Table 23).

An agent set to *RMON-2 Traffic Mode* can still be used for network management by LANsentry® Manager, or any other software which uses the RMON tables.

**Table 23** RMON-1 and RMON-2 Table Sizes that Decrease in Traffic Mode

RMON-1 Table Sizes	RMON-2 Table Sizes
Capture Buffer Packets	User History*
Packet Limit	Higher Layer Host
Total Capture Packets	Higher Layer Matrix

\* The number of interfaces supported also decreases



**CAUTION:** If you change the RMON-2 mode, the agent automatically cold restarts for the changes to take effect. Refer to the *Firmware Upgrade documentation* or your agent documentation for a description of the data lost when an agent is cold restarted. The latest version of the *Firmware Upgrade documentation* is available from the 3Com web site:

<http://www.support.3com.com/infodeli/tools/netmgt/rmonprob/family.htm>.

There are three available modes:

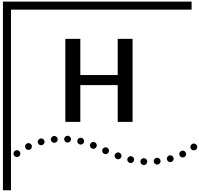
- **Standard Mode** Sets appropriate table sizes on the device for use with a third-party management application.

- **Traffic Mode** Sets appropriate table sizes on the device for use with Traffic Manager.
- **Off** Disables RMON-2. With RMON-2 disabled you can download SmartAgent® software to the device.



*If you disable RMON-2 on an agent which supports both RMON standards, RMON-1 will still be enabled. Traffic Manager can only collect limited data, in the form of line statistics reports, from an agent that supports RMON-1 only. See [Appendix I, "Using RMON-1 Agents"](#) for more information.*





# DHCP

This appendix contains the following sections:

- [How Traffix Manager Monitors DHCP Devices](#)
- [What Effect Do DHCP Devices Have On The Map?](#)

---

## How Traffix Manager Monitors DHCP Devices

Traffix™ Manager normally uses the Network Layer Address (for example, IP address, IPX address) as the unique way to identify objects on your network. However, the IP address of devices managed using the Dynamic Host Control Protocol (DHCP) can change, and therefore this is an unreliable method of identification for these devices.

The only certain way of identifying such devices in the Map is to use the MAC address of the device. You can use the DHCP configuration file to specify which devices you want Traffix Manager to identify using this method. You can open this file by clicking *DHCP Setup* in the Traffix Control Panel.

---


## What Effect Do DHCP Devices Have On The Map?

If a device which is managed using DHCP is discovered on your network, it may appear on the Traffix Manager Map as a normal device until Traffix Manager realizes it is a DHCP device.

A DHCP device requests an IP address from the DHCP server. DHCP is a dynamic protocol, and the DHCP server can provide a different IP address for the same device each time this request is made. If, according to your local DHCP policy, the IP address of a device changes, the device will appear exactly the same in the Map, except that its IP address will change.

If the old IP address of a device is assigned to a new MAC address, a new device is created in the Map. This new device will have the old IP address and the new MAC address attribute assigned to it. The original device

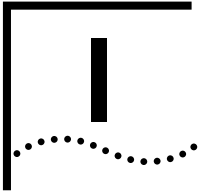
(with the old MAC address) will also remain on the Map. There will therefore be two devices on the Map with the same IP address, although with different MAC addresses. Any conversation data retrieved for this IP address is subsequently assigned to the new device. This continues until the next time Traffix Manager detects that a MAC address has changed.

Therefore, multiple objects can appear in the Map with the same Network Layer address, although with a different MAC address attribute. These are represented by a unique icon. 

Each IP address listed in the DhcpDB file is polled every `<POLLINGINTERVAL>` minutes, using a Netbios NCBSTAT request. This request returns the MAC address of the device, provided the device supports Netbios. Windows-based operating systems and DOS support Netbios, but other systems, such as UNIX, generally do not.



*You can edit the polling interval in the DhcpDB file. However, decreasing the polling interval to less than 30 minutes would not enable Traffix Manager to detect changes in MAC addresses more accurately, as data is only stored at 60-minute granularity.*



# USING RMON-1 AGENTS

---

## Monitoring Network Segments Using RMON-1 Agents

Many sites (particularly in a switched environment) have large numbers of network segments, and it may be too expensive to monitor all segments with RMON-2 agents. You can use any existing embedded RMON-1 only devices (hubs, switches, routers etc.) instead, to produce lightweight activity reports for these segments.



*Data from RMON-1 only agents is only used in segment activity reports, and does not appear in the Map.*

To produce a lightweight segment activity report, follow these steps:

- 1 In the Configure Agents dialog box, add and enable the RMON-1 devices and interfaces you want to use to collect network traffic data.

Traffix™ Manager will automatically begin to collect data from the enabled interfaces.

- 2 From the Report Manager, schedule a daily Segment Activity report for the next morning (weekly and monthly reports can also be scheduled).

When you look at the report, you will find that the following graphs are incomplete:

- Protocol Distribution of Segment By Octets (no data).
- Key to graph with no data — no key is displayed.
- Protocol Distribution By Octets With Packets Overlaid — only the packet overlay appears.

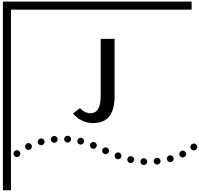
The remaining graphs and tables all appear in full.



*RMON-1 only segments will never appear in a TopN Segments report since the Reporter uses (RMON-2) protocol information to calculate the top N segments.*







# RMON AND SNMP TABLES RETRIEVAL

This appendix lists the SNMP tables retrieved by Traffix™ Manager.

Refer to the following URLs for descriptions of RMON tables:

- RMON-1 Request for Comment:  
<http://www.it.kth.se/docs/rfc/rfcs/rfc1757.txt>
- RMON-2 Request for Comment:  
<http://www.it.kth.se/docs/rfc/rfcs/rfc2021.txt>
- RMON-2 Protocol Identifiers:  
<http://www.it.kth.se/docs/rfc/rfcs/rfc2074.txt>

---

## SNMP Tables used by Traffix Manager

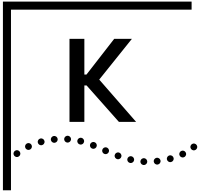
**Table 24** SNMP Tables Used By Traffix Manager

MIB	Table	Mandatory	Comments
MIBII	system	yes	Used to get sysDescr
MIBII	interfaces	yes	Used to get interface list
RMON	probeConfig	no	Used by agentAdmin to reboot probe and download new firmware
RMON	etherStats / trPStats / trMLStats	no	Line statistics (for reports only)
3Com	fddiStats	no	FDDI line statistics (for reports only)
RMON-2	protocolDir	required for RMON-2 data	RMON-2 protocols
RMON-2	probeCapabilities	no	Used to determine which matrix group (al or nl) is supported

(continued)

**Table 24** SNMP Tables Used By Traffic Manager (continued)

<b>MIB</b>	<b>Table</b>	<b>Mandatory</b>	<b>Comments</b>
RMON-2	protoDist	no	For protocol distribution (reports only)
RMON-2	addressMap	no	Network Layer to MAC address mapping
RMON-2	alMatrixTopN / alMatrix / nlMatrixTopN / nlMatrix	At least one must be supported for RMON-2 data	RMON-2 conversation traffic



# TECHNICAL SUPPORT

3Com® provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

---

## Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- [World Wide Web Site](#)
- [3Com Knowledgebase Web Services](#)
- [3Com FTP Site](#)
- [3Com Bulletin Board Service](#)
- [3Com Facts Automated Fax Service](#)

## World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site, enter this URL into your Internet browser:

**<http://www.3com.com/>**

This service provides access to online support information such as technical documentation and software, as well as support options that range from technical education to maintenance and professional services.

## 3Com Knowledgebase Web Services

This interactive tool contains technical product information compiled by 3Com expert technical engineers around the globe. Located on the World Wide Web at **<http://knowledgebase.3com.com>**, this service gives all 3Com customers and partners complementary, round-the-clock access to technical information on most 3Com products.

**3Com FTP Site** Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **ftp.3com.com**
- Username: **anonymous**
- Password: **<your Internet e-mail address>**



*You do not need a user name and password with Web browser software such as Netscape Navigator and Internet Explorer.*

**3Com Bulletin Board Service** The 3Com BBS contains patches, software, and drivers for 3Com products. This service is available through analog modem or digital modem (ISDN) 24 hours a day, 7 days a week.

#### Access by Analog Modem

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	Data Rate	Telephone Number
Australia	Up to 14,400 bps	61 2 9955 2073
Brazil	Up to 28,800 bps	55 11 5181 9666
France	Up to 14,400 bps	33 1 6986 6954
Germany	Up to 28,800 bps	4989 62732 188
Hong Kong	Up to 14,400 bps	852 2537 5601
Italy	Up to 14,400 bps	39 2 27300680
Japan	Up to 14,400 bps	81 3 5977 7977
Mexico	Up to 28,800 bps	52 5 520 7835
P.R. of China	Up to 14,400 bps	86 10 684 92351
Taiwan, R.O.C.	Up to 14,400 bps	886 2 377 5840
U.K.	Up to 28,800 bps	44 1442 438278
U.S.A.	Up to 53,333 bps	1 847 262 6000

### Access by Digital Modem

ISDN users can dial in to the 3Com BBS using a digital modem for fast access up to 64 Kbps. To access the 3Com BBS using ISDN, call the following number:

**1 847 262 6000**

### 3Com Facts Automated Fax Service

The 3Com Facts automated fax service provides technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3Com Facts using your Touch-Tone telephone:

**1 408 727 7021**

---

### Support from Your Network Supplier

If you require additional assistance, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

---

### Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, call the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Here is a list of worldwide technical telephone support numbers:

Country	Telephone Number	Country	Telephone Number
<b>Asia, Pacific Rim</b>			
Australia	1 800 678 515	P.R. of China	10800 61 00137 or 021 6350 1590
Hong Kong	800 933 486	Singapore	800 6161 463
India	+61 2 9937 5085	S. Korea	
Indonesia	001 800 61 009	From anywhere in S. Korea:	00798 611 2230
Japan	0031 61 6439	From Seoul:	(0)2 3455 6455
Malaysia	1800 801 777	Taiwan, R.O.C.	0080 611 261
New Zealand	0800 446 398	Thailand	001 800 611 2000
Pakistan	+61 2 9937 5085		
Philippines	1235 61 266 2602		
<b>Europe</b>			
From anywhere in Europe, call:	+31 (0)30 6029900 phone		
	+31 (0)30 6029999 fax		
<b>Europe, South Africa, and Middle East</b>			
From the following countries, you may use the toll-free numbers:			
Austria	0800 297468	Netherlands	0800 0227788
Belgium	0800 71429	Norway	800 11376
Denmark	800 17309	Poland	00800 3111206
Finland	0800 113153	Portugal	0800 831416
France	0800 917959	South Africa	0800 995014
Germany	0800 1821502	Spain	900 983125
Hungary	00800 12813	Sweden	020 795482
Ireland	1800 553117	Switzerland	0800 55 3072
Israel	1800 9453794	U.K.	0800 966197
Italy	1678 79489		
<b>Latin America</b>			
Argentina	AT&T +800 666 5065	Mexico	01 800 CARE (01 800 2273)
Brazil	0800 13 3266	Peru	AT&T +800 666 5065
Chile	1230 020 0645	Puerto Rico	800 666 5065
Colombia	98012 2127	Venezuela	AT&T +800 666 5065
<b>North America</b>			
	1 800 NET 3Com (1 800 638 3266)		
	Enterprise Customers: 1 800 876-3266		

## Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense.

To obtain an authorization number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	+ 65 543 6500	+ 65 543 6348
Europe, South Africa, and Middle East	+ 31 30 6029900	+ 31 30 6029999
Latin America	1 408 326 2927	1 408 326 3355

From the following countries, you may call the toll-free numbers; select option 2 and then option 2:

Austria	0800 297468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0800 1821502	
Hungary	00800 12813	
Ireland	1800553117	
Israel	1800 9453794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	00800 3111206	
Portugal	0800 831416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266)	1 408 326 7120 (not toll-free)
	Enterprise Customers: 1 800 876 3266	





# GLOSSARY

- agent** A standalone or embedded source of RMON-1 or RMON-2 data.
- aggregation** The process of adding the data from multiple devices in the same domain, and representing those devices as a simple “aggregated” device. Used to limit database growth.
- application** As used in Traffix™ Manager, this is a grouping of related RMON-2 defined protocols. It provides the user with a more recognizable and convenient way of selecting protocols.
- application layer** Layer seven, the uppermost part of the OSI Reference Model. This layer contains the user and application programs.
- ARP** Address Resolution Protocol. ARP is a TCP/IP Interior Gateway Protocol for dynamically mapping Internet addresses to physical hardware addresses on LANs. It is limited to LANs that support hardware broadcast.
- attribute** A label for a piece of information about devices: for example, the location of a device, or its *IP address*. Traffix Manager is supplied with a number of predefined attributes, and you can add your own. See [Chapter 4, “Grouping Network Devices in the Map”](#) for more information about attributes.
- backbone** The part of a network used as the primary path for transporting traffic between network segments.
- bandwidth** Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps and the bandwidth of Gigabit Ethernet is 1000Mbps. FDDI bandwidth is 100 Mbps. Token Ring bandwidth is 4 or 16 Mbps.

- bit** Either of the digits 0 or 1 when used in the binary numeration system. Eight bits equals a single *byte*.
- broadcast** All good frames destined for the broadcast address, in other words sent out to all stations on the network. Some broadcasts are limited to the local network, and some broadcasts may cross onto other networks.
- client** An application that provides a means of configuring data collection. Multiple Traffic Manager clients can be run against a single Traffic Manager server.
- community name** Also known as community string. *SNMP* uses community names to limit access to certain device management functions. The community name used when accessing a device determines which functions may be accessed.
- CSV format file** Comma Separated Value File. Traffic Manager uses raw report data to output reports as CSV files. CSV files can be read into spreadsheets or database applications for further analysis.
- data link layer** The second layer of the OSI Reference Model. This layer is responsible for controlling message traffic.
- default gateway** The *IP address* of a device, usually a router or gateway, to which the probe directs all packets not destined for its subnet.
- device** A generic term used to refer to any device seen on the network, by way of the addresses recorded in the RMON tables.
- device attribute** A piece of information about a device; for example, an attribute could be the device's *IP address*, or the building in which it is kept.
- DHCP** Dynamic Host Configuration Protocol. DHCP is a protocol which allows dynamic allocation of *IP addresses* to devices on a local area network. The system administrator assigns a range of IP addresses to DHCP. Each DHCP-enabled device on the LAN can request an IP address from the DHCP server. DHCP uses a lease concept to respond to a request for an IP address and to grant an IP address to a device. The system administrator can control for how long a client can use a particular IP address.
- DNS** Domain Name Service. A mapping of host names to *IP addresses*. When you enter a destination host name, the station asks the DNS server for the IP address associated with the host name. Upon receipt

of the destination IP address, the station sends the message to the destination station. Due to the static nature of DNS, it can only be used when network stations have static IP addresses obtained through manual configuration, *BOOTP* or *DHCP* in static mode.

- domain** Part of the naming hierarchy used on the Internet and represented by a series of names separated by dots. For example, the domain name `user.net.3com.com` provides the path to a company (`com`) called `3com`, to a company network called `net`, and finally to the destination computer, `user`.
- event** Traffic Manager enables you to configure rules which provide you with information about the traffic on your network and network security. Predefined or configured rules are applied to traffic data as it is collected. When the conditions of a rule are met, an event is generated to alert you to a significant change on your network.
- favorite** A way of specifying *applications* and protocols, so that you can select and view network traffic at higher levels of abstraction. Traffic Manager contains a number of predefined favorites, and you can add your own as required. See [Chapter 7, "Displaying Network Traffic in the Main Window"](#) for more information about setting up favorites.
- firewall** A combination of specifically configured network hardware and software products that limit access to the network by unauthorized individuals from outside the firewall. For example, a firewall can control access between an internal network and the Internet.
- firmware** Software running on an agent or probe.
- group** Term used in Traffic Manager to define a number of devices sorted by common criteria or *device attributes*.
- HTTP** HyperText Transfer Protocol. A protocol used for transferring text and images over an intranet or the Internet.
- IETF** Internet Engineering Task Force, whose responsibilities include specification of protocols and recommendation of Internet standards via the Request for Comment (RFC) process.
- interface** In Traffic Manager, an interface refers to a connection from an agent to the network being monitored.

- IP (network) address** Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network part, identifying which network the device resides on, and a host part, identifying individual devices on a given network.
- IPX** Internetwork Packet Exchange. Network Layer (OSI Layer 3) protocol used for transferring data from servers to workstations.
- MAC address** The hardware address of a device connected to a shared medium.
- Map** Graphical display of your network in the main window of Traffix Manager, showing groups of devices and the traffic connections between them.
- MIB** Management Information Base. In *SNMP*, the MIB is the database where information about the managed objects is stored. The MIB can contain information about many aspects of the devices being managed.
- multicast** A message sent to a specific group of nodes on a network simultaneously.
- NL** Network Layer. The third layer of the OSI Reference Model. This layer is responsible for controlling message traffic. It receives data that has been framed by the Data Link Layer below it, converts this data into packets, and passes the result to the Transport Layer that directs the packets to their destination.
- network sweep attack** If someone from outside your network is attempting to gain access to your network without permission, one technique they may use is to systematically test every IP address on your network in an attempt to discover the address of real devices which can be accessed. For the purpose of the Traffix Manager events system, this is referred to as a network sweep attack.
- object** Term used in Traffix Manager to describe a device or a group of devices displayed in the *Map*.
- Object List** A hierarchical list of the devices and groups of devices seen on your network.
- octet** A digital unit of information comprising eight binary digits (bits) equivalent to a *byte*.

<b>OSI</b>	Open Systems Interconnection, a body of standards set by the International Standards Organization to define the activities that must occur when computers communicate. The OSI Reference Model is a 7-layer framework within which communications protocols and standards have been defined.
<b>packet</b>	A unit of information that contains data, origin information and destination information, which is switched as a whole through a network.
<b>physical layer</b>	The first layer of the OSI Reference Model. This layer manages the transfer of individual bits of data over wires, or whichever medium is used to connect workstations and peripherals.
<b>presentation layer</b>	The sixth layer of the OSI Reference Model. This layer controls the formatting and translation of data.
<b>probe</b>	Standalone RMON-1 or RMON-2 agent responsible for gathering network data on a remote segment and passing it up to a central management station. Usually configured and controlled by the client.
<b>protocol</b>	As used in Traffic Manager, this is the RMON-2 decoding of the type of traffic seen on the network.
<b>protocol number</b>	The port or program number as defined by the parent protocol. For example, if you are adding a TCP child protocol, the protocol number will be the TCP port number.
<b>RMON-1</b>	Remote MONitoring. Subset of <i>SNMP</i> MIB II which allows monitoring and management capabilities by addressing up to ten different groups of information. Defined in <i>IETF</i> document RFC 1757.
<b>RMON-2</b>	Extends the capability of RMON-1 to include protocols above the MAC layer.
<b>segment</b>	For the purposes of the Traffic Manager reporter, a segment is considered to be the interface on a particular agent on your network.
<b>SNMP</b>	Simple Network Management Protocol. A protocol originally designed to be used in managing TCP/IP internets.
<b>subnet mask</b>	A filtering system for <i>IP addresses</i> . It distinguishes the network ID part of an IP address from the host ID part. A subnet mask is a 32-bit number expressed as four decimal numbers, in the range 0 to 255,

separated by periods. Devices and routers use the mask to identify the subnet on which a device resides.

**switch** A device which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

**system descriptor** A free-form field on RMON devices used by vendors to supply basic information about the device.

**TCP** A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer and other services for communication among a wide range of computer equipment.

**TFTP** Trivial File Transfer Protocol. Allows you to transfer files, such as software upgrades and configuration files, to and from a remote device.

**TNCS** Transcend® Network Control Services. A suite of standards-based, integrated management applications for configuring, monitoring and troubleshooting 3Com network systems.

**top N** The top N components of your network are calculated using some appropriate sorting condition such as utilization or by total octets sent and received over a specified period. See [Chapter 11, "Overview of Reporting"](#).

**transport layer** The fourth layer of the *OSI* network layer model. This is responsible for error checking and correction, and some message flow control.

**tree** See *Object List*.

**UDP** User Datagram Protocol. A protocol enabling an application to send individual messages to other applications.

# INDEX

---

## Numbers

3Com Bulletin Board Service (3Com BBS) 164  
3Com Knowledgebase Web Services 163  
3Com URL 163  
3ComFacts 165

---

## A

Access tables

    dblookup program 143

acknowledging events 85

activity reports 89, 99

ad hoc reports 90, 94

Add Agents dialog box 53

adding

    agents 53

    connections between objects 60

    connections to and from objects 60

agent firmware 153

Agent Maintenance dialog box 54, 154

Agent Statistics dialog box 54

agent tree 52

agents

    adding 52, 53

    configuring 52

    deregistering user-defined protocols with 63

    disabling 52

    discovering 52

    downloading firmware 153

    duplicate 53

    editing 52, 53

    enabling 52, 54

    finding 52

    finding automatically using Traffix Manager 52

    finding manually 52

    invalid 53

    mode 154

    registering user-defined protocols with 63

    setting RMON-2 mode on 54

    specifying agent details yourself 52

    supported interface types 151

    supported RMON-2 agents 51

    supported RMON-2 interfaces 51

    viewing agent statistics 54

    which support user-defined protocols 63

aggregating devices

    default aggregation action 131

    local domain specification 130

    local domains 130

    overview 64, 129

    setting maximum device limit 132

    specifying aggregation policy 130

aggregation policy

    specifying 130

application

    definition 61

areas

    locating in Map 59

    zooming to in Map 59

assigning attributes

    automatic 137

    configuration file 138

    dblookup default values 143

    dblookup program 142

    running process 140

    standard programs 138

    writing programs 145

attribute lookup 125

attribute lookup program

    building 147

    examples 147

    structure 145

    writing 147

attribute lookup programs

    library functions 148

    testing 149

attributes

    assigning automatically 137

    creating and assigning 44

    definition 40

    predefined 40

attributes configuration file

    contents 138

    format 139

Attributes dialog box 45

---

**B**

Bulletin Board Service 164

---

**C**

client

- access levels 50
- administrator access 50
- description 37
- launching after the first time 49
- launching for the first time 26
- read-only user 50
- running multiple clients against a single server 50

cold restart

- losing data 154

collecting data

- adding agents 53
- disabling agents 52
- editing agents 53
- enabling agents 52, 54
- polling interval 54
- resuming collection 52, 54
- RMON-1 agents only 38
- suspending collection 52, 54

collector

- overview 35

community names

- definition 53
- overview 53

community strings. *See* community names

configuration files

- automatic attribute assignment 138
- fileattrs 140
- fileattrs examples 140
- format for fileattrs 140

Configure Agents dialog box 52, 54

configuring

- data sources 52
- event rules 75

connection activity report

- contents 100

connections

- between objects 60
- removing 61
- to and from objects 60

Control Panel. *See* Traffix Control Panel

conventions

- notice icons 13
- text 13

creating

- events 20, 36

reports 93

CSV files

description 95

---

**D**

daily reports

- producing 90

data collection

- adding agents 53
- disabling agents 52
- editing agents 53
- enabling agents 52, 54
- polling interval 54
- resuming 52, 54
- RMON-1 agents only 38
- suspending 52, 54

data loss

- cold restart 154

database maintenance 123

Database Maintenance dialog box 123

database schema 121

database setup 122

Database Setup dialog box 122

databases

- cleaning 124
- managing 121 to 126
- optimizing 125
- repairing 124

dblookup program 142

- Access tables 143

database structure 142

default values 143

Excel workbooks 144

Excel worksheets 144

how it works 144

lookup tables 144

running 144

default aggregation action 131

default DNS domain 126

default event rules 72

default gateway

- IP address 170

deinstalling Traffix Manager v2.0 127

deleting

- events 85
- global deletion policy 96
- report data 96
- reports 93

deregistering user-defined protocols with agents 63

deselecting objects in the main window 59

detecting

- network misuse 73, 79



- network sweep attacks 73
- new devices on your network 73
- unauthorized machine access 73
- device activity report
  - contents 101
- device aggregation
  - default aggregation action 131
  - local domain specification 130
  - local domains 130
  - overview 23, 64
  - setting maximum device limit 132
  - specifying aggregation policy 130
- device limit
  - setting 132
- devices
  - assigning attributes 140
  - displayed in graph 29
  - in Map 29
  - in the Object List 28
  - setting RMON-2 mode on 54
  - specifying for an event rule 76
- DHCP
  - effect of DHCP devices on the Map 157
  - how Traffic Manager monitors DHCP devices 157
- DHCP setup 125, 157
  - editing the polling interval 158
- dialog boxes
  - Add Agents 53
  - Agent Maintenance 54, 154
  - Agent Statistics 54
  - Attributes 45
  - Configure Agents 52, 54
  - Database Maintenance 123
  - Database Setup 122
  - Event Generation 86
  - Event List 82
  - Event Rules 76
  - Filter 83
  - Global Report Options 96
  - Graph Panel 66
  - Graph Panel Settings 67
  - Graph Settings 69
  - Groupings 46
  - Launch Graph 68
  - Load Traffic 57
  - Number of Devices 59
  - Output Monitor 96
  - Report Manager 92
  - Report Schedule 94, 95
  - User Authorization 50
- disabling
  - agents 52

- events 85
  - RMON-2 54, 154
- discovering agents 52
- display of data
  - effect on reporting 98
- displaying
  - events in graphs 85
  - events in the Map 85
  - groups and devices in the Object List 29
  - traffic in graphs 65
  - traffic in the Map 59
- DNS aggregation
  - local domain specification 130
  - local domains 130
- DNS domains
  - IP addresses 130
  - subnets 130
- DNS predefined grouping 43
- documentation
  - how to use 11
- duplicate errors
  - agents 53
  - community names 53
  - IP addresses 53

---

## E

- editing
  - agents 52, 53
- enabling
  - agents 52
  - events 85
- Event Generation dialog box 86
- Event List 82
- Event Rules dialog box 76
- events
  - acknowledging 85
  - assigning severities 86
  - benefits for network monitoring 71
  - configuring event rules 75
  - creating 20, 36
  - default event rules 72
  - deleting 85
  - description 36
  - detecting network misuse 73, 79
  - detecting network sweep attacks 73
  - detecting new devices on your network 73
  - detecting unauthorized machine access 73
  - disabling 85
  - displaying in graphs 85
  - displaying in the Map 85
  - displaying traffic in Map that caused event 85
  - enabling 85

- excepting devices or connections from rules 85
- filtering 83
- forwarding as SNMP traps 86
- generating 20, 36
- ignoring devices or connections 85
- modifying 85
- monitoring critical connections 75
- monitoring critical devices 74
- monitoring long term trends 77
- monitoring network resource usage 74
- monitoring network trends 75
- monitoring protocol usage 78
- monitoring server devices 78
- monitoring WAN and backbone links 79
- network security 71, 78
- network traffic 71
- output to CSV file 84
- overview 71
- overview of rule types 72
- predefined event rules 72
- printing 84
- selecting protocols for an event rule 76
- showing detail 85
- sources of events 81
- specifying devices for an event rule 76
- specifying sensitivity of event rules 77
- specifying time filter 77
- summarizing 84
- viewing 81

Excel workbooks

- dblookup program 144

Excel worksheets

- dblookup program 144

---

## F

- favorite
  - definition 61
- fax service (3ComFacts) 165
- fileattns program 140
  - configuration file 140
  - how it works 141
  - running 141
- files
  - lifetime of HTML output 96
  - SubnetsDB 133
  - troubleshooting missing HTML files 117
  - viewing HTML output 95
- Filter dialog box 83
- filtering
  - events in the Event List 83
- finding agents 52

- firmware
  - cold restart 154
  - downloading to agents 153
  - finding files 153
  - RMON-2 functionality 153
  - TFTP server 153
- forwarding events as SNMP traps 86

---

## G

- generating events
  - overview 20, 36
- getting started
  - reporting 97
  - with Traffix Manager 19, 23
- global deletion policy 96
- global report options 96
- Global Report Options dialog box 96
- Graph Panel 66
- Graph Panel Settings dialog box 67
- Graph Settings dialog box 69
- graphs
  - combined with grouping function 65
  - generating graphs for connections displayed in Map 65
  - overview 20, 65
- group activity report
  - contents 102
- grouping
  - combined with reporting function 39
  - definition 42
  - effect on graphs 65
  - filtering by protocol 61
  - subnets 135
- grouping devices
  - in Map 29
  - overview 39
  - predefined attributes 40
  - predefined groupings 43
- Groupings dialog box 46
- groups
  - unassigned 43
- groups in the Object List 28
- guidelines, tips and hints
  - using graphs to identify key objects 97
  - using grouping to focus reports 97

---

## H

- hiding all traffic connections in the Map 61
- hints on using Traffix Manager. *See* guidelines, tips and hints
- how to use the Traffix Manager documentation 11

**HTML**

- can't find HTML files? 117
  - index file 94, 95
  - lifetime of files 96
  - report directory, moving and linking to 94, 95
  - servicing directory to Web server 94, 95
  - troubleshooting 117
  - viewing report output 95
- 

**I**

- interface types
    - supported 51, 151
  - invalid IP addresses 53
  - IP addresses
    - default gateway device 170
    - DNS domains 130
    - invalid 53
- 

**K**

- key to object status in Map 58
- 

**L**

- Launch Graph dialog box 68
  - launching Traffix Manager
    - no data collected 52
  - launching Traffix Manager after the first time
    - launching client 49
    - launching server 49
    - locating a remote server 50
    - overview 49
  - launching Traffix Manager for the first time
    - launching client 26
    - overview 25
  - library functions
    - attribute lookup programs 148
  - Load Traffic dialog box 57
  - loading network traffic data 57
  - local DNS domains
    - subnets 130
  - local domain specification 130
  - local domains 130
  - locating
    - areas in Map 59
    - objects in Map 59
  - lookup tables
    - dblookup program 144
- 

**M**

- MAC and Type predefined grouping 44

**main window**

- displaying traffic 59
    - Graph Panel 29
    - Map 27, 29
    - menu options 29
    - Object List 28
    - overview 28
    - reference to menu options 29
  - management software. *See* firmware
  - managing the Traffix Manager database 121 to 126
  - Map
    - displaying traffic 59, 60
    - effect of DHCP devices 157
    - locating areas 59
    - locating objects 59
    - overview 29
  - maximum device limit
    - setting 132
  - menu options
    - main window 29
  - MIBs 164
  - modifying
    - events 85
    - reports 93
  - monitoring
    - critical connections 75
    - critical devices 74
    - DHCP devices 157
    - long term trends 77
    - network resource usage 74
    - network segments using RMON-1 agents 159
    - network trends 75
    - server devices 78
    - WAN and backbone links 79
  - monthly reports
    - producing 91
  - multiple clients running against a single server 50
- 

**N**

- network monitoring
  - critical connections 75
  - critical devices 74
  - long term trends 77
  - network resource usage 74
  - network trends 75
  - protocol usage 78
  - server devices 78
  - WAN and backbone links 79
- network security rules
  - detecting network misuse 73, 79
  - detecting network sweep attacks 73
  - detecting new devices on your network 73

- detecting unauthorized machine access 73
  - general rules 78
- network supplier support 165
- network traffic
  - typical 36
- network traffic rules
  - configuring events 71
  - monitoring critical connections 75
  - monitoring critical devices 74
  - monitoring long term trends 77
  - monitoring network resource usage 74
  - monitoring network trends 75
  - monitoring protocol usage 78
  - monitoring server devices 78
  - monitoring WAN and backbone links 79
  - typical network traffic levels 36
- networking, related documentation 14
- new user
  - getting started with Traffix Manager 23
- Number of Devices dialog box 59

---

## O

- Object List
  - description 28
  - viewing groups and devices 29
- object status key 58
- objects
  - adding connections between 60
  - adding connections to and from 60
  - definition 28
  - displaying connections between 60
  - displaying connections to and from 60
  - displaying information about 58
  - displaying object name 58
  - displaying object status 58
  - hiding all connections in the Map 61
  - identifying using MAC address 157
  - identifying using NL address 157
  - locating in Map 59
  - removing all connections 60
  - removing all connections from 61
  - removing connections between 60
  - removing connections to and from 60
  - searching for 59
  - selecting and deselecting in the main window 59
  - statistics 59
  - zooming to in Map 59
- online technical services 163
- Output Monitor dialog box 96
- overviews
  - collector 35

- device aggregation 23
- events 20, 36, 71
- graphs 20, 65
- grouping devices in the Map 39
- launching Traffix Manager after the first time 49
- launching Traffix Manager for the first time 25, 26
- main window 27
- reporting 20, 89
- RMON standards 37
- RMON-2 21, 37

---

## P

- polling for data collection 27, 54
- predefined attributes 40
- predefined event rules 72
- predefined groupings 43
  - DNS 43
  - MAC and Type 44
  - Type and Network 43
  - Vendor and MAC 44
- printing reports 95
- program structure
  - attribute lookup 145
- programs
  - dblookup 142
  - fileattrs 140
  - SubnetsDB 133
- protocols
  - applications and favorites 61
  - deregistering with agents 63
  - filtering display of Map 61
  - monitoring usage 78
  - notes on user-defined protocols 63
  - registering with agents 63
  - selecting for an event rule 76
  - user-defined 62

---

## R

- raw report data
  - overview 93
  - troubleshooting 117
- recommended RMON table sizes 154
- registering user-defined protocols with agents 63
- related documentation
  - networking 14
- remote access 37
- remote monitoring 37
- remote server 50
- removing all traffic connections in the Map 61

- report directory
  - linking to HTML reports 94, 95
- report formats 96
- report instances
  - overview 93
- Report Manager 92
  - displaying information about output status 92
  - displaying information about raw data 92
  - displaying information about report instances 92
  - interpreting raw data and HTML output 94
  - interpreting summary information 94
  - regenerating output 92
  - report instances 93
  - rescheduling reports 92
  - running report generation 92
  - viewing report status 95
- report output 90, 94, 95
- Report Schedule dialog box 94, 95
- report types 89, 99
  - activity reports 89, 99
  - connection activity report 100
  - device activity report 101
  - group activity report 102
  - segment activity report 103
  - top N connections report 105
  - top N devices report 107
  - top N groups report 109
  - top N reports 90, 99
  - top N segments report 110
- reporter options
  - global policies 96
- reporting
  - ad hoc reports 90, 94
  - client access levels 93
  - creating HTML files 95
  - creating reports 93
  - CSV output 90
  - daily reports 90
  - deleting reports 93
  - displaying information about raw report data 92
  - effect of data processing and display 98
  - getting started 97
  - global deletion policy 96
  - guidelines, tips and hints on reporting 97
  - header and footer options 96
  - how long does report generation take? 97
  - HTML output 90, 94
  - interpreting raw data and HTML output 94
  - interpreting summary information 94
  - modifying reports 93
  - monitoring generation and output 96
  - monthly reports 91
  - overview 89
  - periods covered by reports 90
  - printing reports 90, 95
  - raw report data 93
  - report formats 96
  - report instances 93, 94
  - Report Manager 92
  - report output 90, 94, 95
  - saving report contents to CSV files 95
  - scheduling reports 90, 92, 94
  - tools 20
  - troubleshooting 116 to 119
  - viewing report status 95
  - weekly reports 91
- reporting scenarios 97
- reports
  - ad hoc 90, 94
  - connection activity 100
  - device activity 101
  - group activity 102
  - segment activity 103, 159
  - top N connections 105
  - top N devices 107
  - top N groups 109
  - top N segments 110
- resuming data collection 52, 54
- returning products for repair 167
- RFCs
  - 1757 37
  - 2021 37
  - 2074 37
- RMON
  - advantages 37
  - overview 37
  - recommended table sizes 154
  - setting table sizes 154
  - tables retrieval 161
  - URLs 38
- RMON-1
  - configuring RMON-1 data sources 52
  - data collected 38
  - monitoring network segments 159
  - producing segment activity reports 159
- RMON-2
  - changing mode 154
  - configuring RMON-2 data sources 52
  - disabling 54, 154
  - discovering network devices using 38
  - firmware 153
  - overview 21, 37
  - setting mode on agent 54
  - supported agents 151
  - supported interface types 151
  - supported RMON-2 agents and interfaces 51

RMON-2 Standard mode  
 description 154  
 setting 54  
 RMON-2 Traffic mode  
 description 154  
 setting 54  
 rules. *See* events  
 running multiple clients against a single server 50

---

## S

scenarios  
 reporting 97  
 scheduling reports 90, 92, 94  
 searching for objects in the main window 59  
 security  
 configuring events 71  
 detecting network misuse 73, 79  
 detecting network sweep attacks 73  
 detecting new devices on your network 73  
 detecting unauthorized machine access 73  
 rules for enforcing corporate policy about  
 network usage 78  
 rules for maintaining network security 78  
 segment activity report  
 contents 103  
 producing using RMON-1 159  
 selecting objects in the main window 59  
 sensitivity of event rules 77  
 setting  
 maximum device limit 132  
 RMON table sizes 154  
 RMON-2 mode 54  
 RMON-2 Standard mode 54  
 RMON-2 Traffic mode 54  
 subnets 133  
 setting up events 36  
 SNMP  
 tables retrieval 161  
 SNMP traps  
 forwarding events 86  
 sources of events 81  
 specifying aggregation policy 130  
 starting Traffix Manager. *See* launching  
 startup options 125  
 stopping Traffix Manager 28  
 structure of User Guide 19  
 subnets  
 grouping 135  
 local DNS domains 130  
 setting up 133  
 subnets editor 125  
 SubnetsDB file 133

SubnetsDB program 133  
 summarizing events 84  
 suspending data collection 52, 54

---

## T

technical support  
 3Com Knowledgebase Web Services 163  
 3Com URL 163  
 Bulletin Board Service 164  
 fax service 165  
 network suppliers 165  
 product repair 167  
 testing  
 attribute lookup programs 149  
 TFTP server  
 firmware files 153  
 tips on using Traffix Manager. *See* guidelines, tips  
 and hints  
 top N connections report  
 contents 105  
 examples 105  
 how to use 105  
 top N devices report  
 contents 107  
 examples 107  
 top N groups report  
 contents 109  
 examples 109  
 top N reports 90, 99  
 generating summary reports 98  
 top N segments report  
 contents 110  
 traffic rules  
 monitoring critical connections 75  
 monitoring critical devices 74  
 monitoring network resource usage 74  
 monitoring network trends 75  
 Traffix Control Panel  
 attribute lookup 125  
 clean databases 124  
 database applications 122 to 126  
 database maintenance 123  
 database schema 121  
 database setup 122  
 default DNS domain 126  
 DHCP setup 125, 157  
 optimize databases 125  
 overview 121 to 122  
 repair databases 124  
 startup options 125  
 subnets editor 125

Traffix Manager

- assigning attributes automatically 137
- database management 121 to 126
- features 20
- getting started 19, 23
- how it works 21
- how to use the documentation 11
- launching after the first time 49
- launching for the first time 25
- launching with no data collected 52
- main window 27, 28
- menu options 29
- monitoring DHCP devices 157
- RMON tables retrieval 161
- SNMP tables retrieval 161
- starting. *See* launching
- stopping 28
- troubleshooting 115 to 119

Traffix Manager client

- launching after the first time 49
- launching for the first time 26

Traffix Manager server

- launching after the first time 49

Traffix Manager v2.0

- deinstalling 127
- upgrading 126

troubleshooting

- HTML output 117
- raw report data 117
- reporting 116 to 119
- Traffix Manager 115 to 119

Type and Network predefined grouping 43

types of event rule

- detecting network misuse 73
- detecting network sweep attacks 73
- detecting new devices on your network 73
- detecting unauthorized machine access 73
- monitoring critical connections 75
- monitoring critical devices 74
- monitoring network resource usage 74
- monitoring network trends 75
- overview 72

---

## U

unassigned groups 43

upgrading Traffix Manager v2.0 126

URL 163

URLs

- RMON 38

User Authorization dialog box 50

User Guide

- structure 19

user-defined protocols 62

- agents supporting user-defined protocols 63
- deregistering with agents 63
- notes on 63
- registering with agents 63
- RMON-2 limitations 63

---

## V

Vendor and MAC predefined grouping 44

viewing

- agent statistics 54
- events 81
- groups and devices in the Object List 29
- sources of events 81

---

## W

Web server

- index file 94, 95
- serving HTML directory 94, 95

weekly reports

- producing 91

where to find specific information in the documentation 11

World Wide Web (WWW) 163

- networking sites 14

---

## Y

year 2000 compliance 16

---

## Z

zooming

- zoom in 31
- zoom out 31
- zoom to 31

zooming to areas in Map 59

zooming to objects in Map 59





# 3Com Corporation LIMITED WARRANTY

## Transcend® Traffix™ Manager 3.0 for Windows NT®

---

### SOFTWARE

3Com warrants that each software program licensed from it will perform in substantial conformance to its program specifications, for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with 3Com's published specifications or user manual.

---

### YEAR 2000 WARRANTY

In addition to the Software Warranty stated above, 3Com warrants that each product sold or licensed to Customer on and after January 1, 1998 that is date sensitive will continue performing properly with regard to such date data on and after January 1, 2000, provided that all other products used by Customer in connection or combination with the 3Com product, including hardware, software, and firmware, accurately exchange date data with the 3Com product, with the exception of those products identified at 3Com's Web site, <http://www.3com.com/products/yr2000.html>, as not meeting this standard. If it appears that any product that is stated to meet this standard does not perform properly with regard to such date data on and after January 1, 2000, and Customer notifies 3Com before the later of April 1, 2000, or ninety (90) days after purchase of the product from 3Com or its authorized reseller, 3Com shall, at its option and expense, provide a software update which would effect the proper performance of such product, repair such product, deliver to Customer an equivalent product to replace such product, or if none of the foregoing is feasible, refund to Customer the purchase price paid for such product.

Any software update or replaced or repaired product will carry a Year 2000 Warranty for ninety (90) days after purchase or until April 1, 2000, whichever is later.

---

### OBTAINING WARRANTY SERVICE

Customer must contact a 3Com Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from 3Com or its authorized reseller may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after 3Com receives the defective product.

*Dead- or Defective-on-Arrival.* In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than thirty (30) days after the date of purchase, and this is verified by 3Com, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided by advance replacement. The replacement product will normally be shipped not later than three (3) business days after 3Com's verification of the DOA product, but may be delayed due to export or import procedures. When an advance replacement is provided and Customer fails to return the original product to 3Com within fifteen (15) days after shipment of the replacement, 3Com will charge Customer for the replacement product, at list price.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

---

### WARRANTIES EXCLUSIVE

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT

THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS, OR ACTS OF GOD.

---

**LIMITATION OF LIABILITY**

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

---

**DISCLAIMER**

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

---

**GOVERNING LAW**

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

**3Com Corporation**  
5400 Bayfront Plaza  
Santa Clara, CA 95054  
(408) 326-5000